1. AMAÇ:

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde gerçekleşen Bilgi güvenliği ihlal olaylarını ve fark edilen zayıflıkları zamanında kayıt altına almak ve haberdar olmak, güvenlik ihlallerine yanıt vermek, ihlal ve zayıflıklara karşı faaliyet planları oluşturmak ve edinilen bilgilerle tehditlere karşı önleyici tedbirler almaktır.

2. KAPSAM:

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığındaki tüm ihlal olay yönetimi kontrollerini kapsar.

3. YASAL DAYANAK: -

4. SORUMLULAR:

Bilgi İşlem Daire Başkanı, Şube Müdürü ve Üst Yönetim bilgi güvenliği olaylarının engellenmesi ve zayıflıkların ortadan kaldırılması için yatırım desteği sağlar.

Tüm personel bilgi güvenliği olayı gerçekleştiğinde ya da bilgi güvenliği konusunda bir zayıflığı tespit ettiğinde BGYS temsilcisine bildirir.

BGYS temsilcisi olayların kayıt edilmesi, raporlanması ve faaliyetlerin planlanarak gerçekleştirilmesi işlemlerini yönetir.

5. UYGULAMA

Tanımlar:

Kişisel Veri: Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder.

Özel Nitelikli Kişisel Veri: Özel nitelikli kişisel veriler, islenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına neden olma riski taşıyan verilerdir.

Bilgi Güvenliği İhlal Olaylarının, Zayıflıkların ve tehditlerin fark edilmesi

Oryantasyon eğitimlerinin bir parçası olarak, bilgi güvenliği farkındalık eğitimlerinde ve Bilgi İşlem Daire Başkanlığı ortak sunum alanlarında (sunum sistemi, panolar vb.) bilgi güvenliğine yönelik zayıflıklar, tehditler ve ihlal olaylarına yer verilecek ve personel bilgilendirilecektir.
Aşağıda belirtilen ihlallerin ve bunların dışında fark edilen zayıflıkların bildirilmesi ve gerçekleşmesi durumunda bilgi güvenliği ihlal olay yönetimi tetiklenecektir**.**

Uygunsuz Kullanım **:** Varlıkların ve hizmetlerin amacı dışında kullanımı. Temiz Masa ve Temiz Ekran talimatlarına uyulmaması.

Zararlı Kodlar **:**Virüs vb. kötü niyetli kodların sistemi çalışmaz hale getirmesi, ya da süreci yavaşlatması.

Hizmet Dışı Kalma : Sistemin (Sunucu, internet, CRM vb.) tümüyle çalışmaz hale gelmesi.
Yetkisiz Erişim : Kişinin yetkisi dışında bilgi ve fiziksel varlıklara erişmesi.

Olayın BGYS Temsilcisine İletilmesi ve Kayıt edilmesi

İhlaller herhangi bir personel tarafından fark edildiği anda BGYS temsilcisine ulusome@uludag.edu.tr adresine mail yoluyla bildirilecektir. Yönetim temsilcisi ve ekip kararı doğrultusunda olay ihlali olduğu kararı verilirse Bilgi Güvenliği Olay İhlal Formu ile kayıt altına alınır.

Bilgi Güvenliği İhlal Olaylarına Yanıt Verilmesi

Bilgi güvenliği ihlali olay durumunda BGYS yönetim temsilcisi ya da ekip personeli aşağıda belirtildiği şekilde hareket edilmesini sağlar;
-İlgili sistemin ya da faaliyetin durdurulması,
-Zarar görmüş ya da zararı yaygınlaştırabilecek sistemlerin yalıtılarak müdahale edilmesi, ilgili bilgisayar ağının kapatılması,
-Fiziksel durumlarda güvenlik ekiplerine bilgi verilerek gerekli önlemlerin alınması, firmaya giriş ve çıkışların durdurulması,
-Üst yönetime bilgi verilmesi,
-Fotoğraf ve belgelerle kanıt toplanması sağlanacaktır.

Olay İhlallerinde Kanıt Toplama

Delillerin değişmesine ya da bozulmasına imkân tanımamak amacıyla, olay yerinin güvenliği sağlanmalıdır. Çevre güvenliğinin asıl amacı delilleri korumaktır. Bu aşamada olay yerine giriş kontrol altına alınmalı, giren ve çıkan kişilerin kaydı tutulmalı ve amaçsız bir şekilde olay mahallinde bulunulmasına izin verilmemelidir. Özellikle, dışarıya çıkan kişilerin üzerinde herhangi bir materyalin bulunmadığından emin olunmalıdır.
Fiziksel ve çevresel olay ihlallerinde kanıt olarak fotoğraf ve/veya video çekilebilir ve olay ihlal bildirim formuna ek delil olarak kullanılabilir. Olay ihlali yaşanan bölge kamera izleme bölgesinde ise kamera kayıtlarının bir kopyası güvenli bir ortama alınmalıdır.

SORUMLU PERSONEL (Tebellüğ Eden)	KONTROL EDEN	ONAYLAYAN (Tebliğ Eden)

Yaşanan olay ihlali işletim sistemleri/dijital ortam üzerinde ise ilk işlem olarak sistemin gölge kopyasının alınması gerekmektedir. Log tutan cihazlarda yaşandığı taktirde ilgili log kayıtlarının zaman kaybedilmeden güvenli bir ortama kopyası alınmalıdır.

Referanslar

- TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
- TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları
- İhlal bildirim formu.

SORUMLU PERSONEL (Tebellüğ Eden)	KONTROL EDEN	ONAYLAYAN (Tebliğ Eden)