İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1. Amaç

Bu prosedürün amacı ESOGÜ bünyesinde kullanılan bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemlere yönelik anti-virüs kullanım esaslarının tanımlanmasıdır.

2. Kapsam

ESOGÜ bünyesinde kullanılan tüm bilgisayarlar, kötücül yazılımların tehdidinde olan tüm sistemler ve bunları kullanan personel bu politika kapsamındadır.

3. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Uygulanmasından sorumluluğundan herhangi bir bilgisayar veya kötücül yazılımların tehdidinde olan sistemleri kullanan personel sorumludur.

5. Uygulama

Tanımlama: Politika maddeleri anlatılırken bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemler için genel olarak "bilgisayar" ifadesi kullanılacaktır.

- Kurumumuzun veya hizmet verdiğimiz kullanıcıların bütün bilgisayarlar, sunucular vs. sistemlerinde anti-virüs yazılımı yüklüdür.
- Sunucu sistemleri ve kullanıcı bilgisayarları zararlı yazılımlara karşı düzenli olarak taranır.
- Anti-virüs yazılımları gerçek zamanlı (real time) koruma sağlayacak şekilde konfigüre edilir.
- Anti- virüs yazılımı ve virüs tanımları otomatik olarak güncellenmektedir.
- Anti-virüs yazılımı yüklü olmayan bilgisayarlar ağa bağlanamaz.
- Grup Başkanı/Yöneticisi ve onların özel bir amaç için görevlendirdiği kişiler dışında hiçbir personel tarafından geçici olarak da olsa devre dışı bırakılamaz.
- Anti-virüs yazılımının devre dışı bırakıldığı zamanlarda başka önlemler alınır.

- Anti-virüs yazılımlarının veri tabanları güncellemeleri otomatik olarak yapılır.
- Virüs bulaşan makineler yayılma durumuna karşı kesinlikle kurum ortak ağından çıkarılmalı tam olarak temizleninceye kadar ağa bağlanmaz.
- Bilgisayarlar belirlenmiş periyotlarla 6 ayı geçmeyecek sürelerde cihaz kullanım sorumlusu olan kişi tarafından anti-virüs yazılımı ile taranır.
- Bilgisayarlara takılan taşınabilir aygıtlar her takılmada anti-virüs yazılımı tarafından taranır.
- E-posta sunucusu mail yoluyla virüs ve benzeri tehditlerin sisteme dâhil olması durumu için kritik noktada olduğundan fazladan koruma içermelidir. Bilinmeyen veya şüpheli web sitelerinden asla dosya indirilmemelidir.
- Gerekmedikçe klasörleri, dosyaları veya diskleri paylaşıma açma, okuma/yazma yetkileri verilmemelidir.
- Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmaması, kaydedilmemesi ve aktarılmaması gerekir.
- İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilir.
- Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılır.

6. Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7. İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI