# İÇİNDEKİLER

[İÇİNDEKİLER 1](#_Toc533586937)

[1 Amaç 2](#_Toc533586938)

[2 Kapsam 2](#_Toc533586939)

[3 Sorumlular 2](#_Toc533586940)

[4 Uygulama 2](#_Toc533586941)

[5 Yaptırım 3](#_Toc533586942)

[6 İlgili Dokümanlar 3](#_Toc533586943)

# Amaç

Bu politikanın amacı Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kullanılan bilgisayarlar ve kötücül yazılımların tehdidinde olan tüm sistemlere yönelik anti-virüs kullanım esaslarının tanımlanmasıdır.

# Kapsam

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kullanılan tüm bilgisayarlar, kötücül yazılımların tehdidinde olan tüm sistemler ve bunları kullanan personel bu politika kapsamındadır.

# Sorumlular

Bu politikanın oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Uygulanmasından sorumluluğundan herhangi bir bilgisayar veya kötücül yazılımların tehdidinde olan sistemleri kullanan personeller sorumludur.

# 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. Windows işletim sistemlerinde anti-virüs yazılımı yüklü olmalıdır.
* Anti-virüs yazılımları gerçek zamanlı (real time) koruma sağlayacak şekilde konfigüre edilmelidir.
* Anti- virüs yazılımı ve virüs tanımları otomatik olarak güncellenmelidir.
* Anti-virüs yazılımı yüklü olmayan bilgisayarlar ağa bağlanmamalıdır.
* Grup Başkanı/Yöneticisi ve onların özel bir amaç için görevlendirdiği kişiler dışında hiçbir personel tarafından geçici olarak da olsa devre dışı bırakılmamalıdır.
* Anti-virüs yazılımının devre dışı bırakıldığı zamanlarda başka önlemler alınmalıdır.
* Anti-virüs yazılımlarının veri tabanları güncellemeleri otomatik olarak yapılmalıdır.
* Virüs bulaşan makineler yayılma durumuna karşı kesinlikle kurum ortak ağından çıkarılmalı tam olarak temizleninceye kadar ağa bağlanmamalıdır.
* Bilgisayarlar belirlenmiş periyotlarla 6 ayı geçmeyecek sürelerde cihaz kullanım sorumlusu olan kişi tarafından anti-virüs yazılımı ile taranmalıdır.
* Bilgisayarlara takılan taşınabilir aygıtlar her takılmada anti-virüs yazılımı tarafından taranmalıdır.
* 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.

# Yaptırım

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

# İlgili Dokümanlar

EYS-PR.021 - DİSİPLİN PROSEDÜRÜ