	TNKÜ **ANTİ-VİRÜS KULLANIM POLİTİKASI**	Doküman No:	EYS-PO-006
		Hazırlama Tarihi:	07.09.2018
		Revizyon Tarihi:	14.08.2025
		Revizyon No:	2
		Toplam Sayfa Sayısı:	2

1 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.

2 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.

3 SORUMLULAR

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

4 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.

5 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PR.021 - DİSİPLİN PROSEDÜRÜ