	POLİTİKA	**DOKÜMAN NO**	BGYS.PLT.03
		YAYIN TAR.	07.01.2019
		REVİZYON NO	03
		REVİZYON TARİHİ	08.04.2025
KONU	AFYON KOCATEPE ÜNİVERSİTESİ ANTİVİRÜS POLİTİKASI		

Revizyon Takip Tablosu		
Revizyon No	**Revizyon Tarihi**	**Revizyon Nedeni**
1	07.01.2023	İlk Yayın
2	11.12.2023	ISO27001:2022 standardına uyum
3	08.04.2025	Cumhurbaşkanlığı BİG Rehberi kapsamında uyum süreci

1. AMAÇ

(1) Bu Politikanın amacı, Afyon Kocatepe Üniversitesinde kullanılan elektronik bilgi araçlarının virüs saldırılarına karşı korunmasına yönelik politikalar ile usul ve esasları düzenlemektir.

2. TANIMLAR

(1) Bu Politikada geçen;

a) Bilgi İşlem Daire Başkanlığı: Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığını,

b) Kullanıcı: Afyon Kocatepe Üniversitesindeki elektronik bilgi araçlarını kullanan üniversitenin tüm personelini, kayıtlı öğrenciyi veya geçici olarak üniversite bünyesinde bulunan kişiyi,

c) Kurum: Afyon Kocatepe Üniversitesini,

ifade eder.

3. KAPSAM

(1) Bu Politika, kurumda kullanılan elektronik bilgi araçlarının içeriden ve dışarıdan gelebilecek virüs saldırılarına karşı korunmasına ilişkin politikalar ile usul ve esasları kapsar.

4. POLİTİKALAR

(1) Kurumda kullanılan elektronik bilgi araçlarının tümünde kurumun temin ettiği antivirüs yazılımı kurulur. Antivirüs yazılımının kurulum süreçleri ve güncellemeleri Bilgi İşlem Daire Başkanlığı tarafından yapılır ve imza veri tabanları sürekli olarak güncel tutulur.[1]

(2) Virüs bulaştığı tespit edilen ve şüphelenilen cihazlar tamamen temizlenene kadar kurum ağından çıkarılır. [2]

(3) Bilgi İşlem Daire Başkanlığı tarafından kurumdaki elektronik bilgi araçlarına kurulacak antivirüs yazılımının işletilmesi ve virüs bulaşan cihazlar ile ilgili prosedür hazırlanır.

(4) Kullanıcıların hiçbiri Bilgi İşlem Daire Başkanlığının izni olmaksızın kurumda kullanılan elektronik bilgi araçlarına Bilgi İşlem Daire Başkanlığı tarafından kurulan antivirüs programını sistemden kaldıramaz.[4]

5. USUL VE ESASLAR

(1) Kurumdaki elektronik bilgi araçlarının virüs saldırılarına karşı korunmasında kullanıcılar ile ilgili usul ve esaslar şunlardır:

a) Kullanıcılar bilinmeyen kaynaklardan gelen hiçbir dosyayı açmamalıdır. Eğer bir dosyanın zararlı olduğundan şüphelenildiyse bu dosyayı hemen silmeli, kullanılan sistemde varsa çöp kutusu veya geri dönüşüm kutusunu da temizlemelidir.[5]

b) Kullanıcılar, bilinmeyen ve şüpheli kaynaklardan kesinlikle dosya indirmemelidir.

c) Kullanıcılar, kurumun elektronik bilgi araçları üzerinde lisanslı, zararsız ve yasal yazılımları kullanmalıdır.

(2) Kurumdaki elektronik bilgi araçlarının virüs saldırılarına karşı korunmasında kurum ile ilgili usul ve esaslar şunlardır:

a) E-posta ile iletilen dosyalar otomatik olarak sistemler ile taranmalıdır. Tarama işlemi ağa giriş, e-posta sistemine giriş, kullanıcı cihazı gibi farklı noktalarda ayrı ayrı yapılmalıdır.[7]

b) Ziyaret edilen internet sayfaları zararlı yazılım taramasından geçirilmelidir.[8]

c) Antivirüs yazılımında cihaz risk düzeyine göre farklı profiller belirlenmelidir.[9]

ç) Ağ üzerinden veya taşınabilir dosya ortamları (CD, DVD, manyetik veya taşınabilir diskler gibi) ile gelen tüm dosyalar antivirüs taramasından geçirilmelidir.[10]

d) Kritik veri ve sistem konfigürasyonları düzenli aralıklar ile yedeklenmeli ve güvenli bir yerde depolanmalıdır.[11]

e) Bilinen veya şüphelenilen ağ sayfalarına erişim engellenmelidir.[13]

f) Kurum sistemleri yazılım ve dosya değişikliklerine karşı düzenli olarak kontrol edilmelidir.[14]

g) Zararlı yazılımların yol açacağı zararlara karşı iş sürekliliği planı hazırlanmalıdır.[16]

ğ) Zararlı yazılımların bulaşması sonucu yıkıcı sonuçların çıkacağı sistemler veya elektronik bilgi araçları diğer sistemlerden izole olarak çalıştırılmalıdır. [17]

h) Kullanıcıya zararlı yazılımlara karşı korunma yöntemleri hakkında eğitim verilmelidir. [18]

ı) Kurum sistemlerinin zarar görmesini, zararlı yazılımların yayılmasını ve iş süreçlerinin kesintiye uğramasını önlemek amacıyla Bilgi İşlem Daire Başkanlığından prosedür hazırlanmalı ve personel görevlendirilmelidir.

(3) Kurumdaki elektronik bilgi araçlarının virüs saldırılarına karşı korunmasında Bilgi İşlem Daire Başkanlığı personeli ile ilgili usul ve esaslar şunlardır:

a) Acil olduğunu tespit ettiği durumlarda herhangi bir onay almaksızın kurumdaki elektronik bilgi araçlarının ağ bağlantısını kesebilir ve elektronik bilgi araçları üzerinde zararlı yazılım analizi yapabilir. Yapılan işlemler hakkında bağlı olduğu yöneticisine gecikmeksizin bilgi verir.[15]

b) Güvenilir kaynaklardan güvenlik bildirimleri ile duyuruları takip etmeli ve değerlendirmelidir. [19]

6. YAPTIRIM

(1) Bu Politikaya aykırı hareket eden kullanıcılar hakkında mevzuatta belirtilen hükümler ve disiplin prosedürü uygulanır.

Hazırlayan	Kontrol Eden	Onaylayan
BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetici (Rektör)