	POLİTİKA	SAYFA NO	1/2
		DOKÜMAN NO	BGYS.PLT.15
		YAYIN TAR.	07.01.2019
		REVİZYON NO	01
		REVİZYON TARİHİ	06.03.2023
KONU	SİBER SALDIRI POLİTİKASI		

Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
01	06.03.2023	Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.

1. AMAÇ

Bu doküman bilişim ortamlarındaki virüs, solucan, truva atı ve diğer zararlı kodlara ve saldırılara karşı Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı kuruluş politikasını tanımlamaktadır.

2. KAPSAM

Bu politika, zararlı kodların bulaştığı tüm bilişim ortamlarını, elektronik iletişim medyasını ve depolama ortamlarını kapsar.

3. UYGULAMA

1. Tüm bilgisayarlar, **Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı** yönetimi tarafından onaylanmış en son antivirüs yazılımları ile koruma altına alınacaktır.

2. Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta mesaj ve ekleri açılmayacaktır.

3. Bilgisayarlarda kullanılan tüm taşınabilir medya ortamları (disket sürücü, Flash ROM, CD-ROM vs.) kullanılmadan önce virüs taramasına tabi tutulacaktır.

4. Tüm e-posta sunucuları için antivirüs koruma yazılımı yüklenecek; tüm e-posta ve ekleri işlem öncesi antivirüs taramasından geçirilecektir.

5. Antivirüs yazılımının tüm güncel imzaları merkezi olarak antivirüs firmasının onaylı sunucusundan otomatik olarak yüklenecek ve ilgili sunuculara dağıtımı yapılacaktır.

6. Internet üzerinden kaynağı belli olmayan web sitesinden yazılım yüklemesi yapılmayacaktır.

Revizyon Nedeni:	**Hazırlayan**	**Kontrol Eden**	**Onaylayan**
Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.	BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetim Rektör

7. Kurum Sistem Uzmanı tarafından siber saldırılarla mücadele için kullanılması yasaklanan ve Kurum içinde duyurulan yazılım ve bileşenleri hiçbir personel tarafından kullanılmayacaktır.

8. Kurum, kuruluş ağına bağlanması gerekli olan **Kurum** dışı istemci ve taşınabilir bilgisayarları ağa DMZ (Demilitarized Zone) ile bağlanmaktadırlar.

9. Kurum personeli, e-posta veya başka yollarla kendilerine gelen ve kendilerinden istenen parola, kullanıcı kimlik veya gizli bilgileri iletmeyecek ve böyle durumlar olursa bunu Kurum Sistem Uzmanına ivedilikle bildirecektir.

10. Kurum personeli, kendi bilgisayarlarından **Kurum** tarafından kurulmuş olan anti virüs ve SPAM koruma yazılımlarını devre dışı bırakamaz veya kaldıramaz.

11. Kurum bilişim ağına etkileşimli olarak bağlanacak herhangi bir bilgisayar sisteminin virüs, truva atı, solucan veya diğer zararlı kod bulunmadığı tespit edildikten sonra bağlantısı gerçekleştirilecektir.

12. Kurum ağı ve önemli sunucu bileşenleri için Ağ ve Sunucu Saldırı Tespit sistemleri devreye alınacaktır.

13. Siber saldırı olması durumunda güvenlik duvarı bağlantıları engelleyecektir.

4. YAPTIRIM

Bu politikaya uygun olarak davranmayan kullanıcılar hakkında mevzuatlarda belirtilen hükümler ve kurumun disiplin prosedürü uygulanır.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.	BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetim Rektör