1. AMAÇ

Bu doküman bilişim ortamlarındaki virüs, solucan, truva atı ve diğer zararlı kodlara ve saldırılara karşı politikanın tanımlamasını amaçlamaktadır.

2. KAPSAM

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

3. SORUMLULUK

Uşak Üniversitesinin tüm çalışanları sorumludur.

4. UYGULAMA

1. Tüm bilgisayarlar, **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** 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 ve ekleri antivirüs taramasından geçirilecektir.

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

6. **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** Sistem Yöneticisi tarafından siber saldırılarla mücadele amacıyla kullanılması yasaklanan ve duyurulan yazılım ve bileşenler hiçbir personel tarafından kullanılmayacaktır.

7. **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** ağına dışarıdan bağlanması gerekli olan kişiler ağa VPN kullanarak bağlanmaktadırlar.

8. **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** personeli, e-posta veya başka yollarla kendilerine gelen ve kendilerinden istenen parola, kullanıcı kimlik veya gizli bilgileri iletmeyecek ve böyle durumlar olursa bunu **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** Sistem Yöneticisine ivedilikle bildirecektir.

9. **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** personeli, kendi bilgisayarlarından **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** tarafından kurulmuş olan antivirüs veya spam koruma yazılımlarını devre dışı bırakamaz veya kaldıramaz.

10. **Uşak Üniversitesi Bilgi İşlem Daire Başkanlığı** ağı ve önemli sunucu bileşenleri için Ağ ve Sunucu Saldırı Tespit sistemleri devreye alınacaktır.

11. Siber saldırı olması durumunda güvenlik duvarı bağlantıları engelleyecektir.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

Hazırlayan	Kontrol	Onay
Ali AKBULUT	Merter KARACAN	Dr. Veli ÇAPALI