



ÇANKIRI KARATEKİN ÜNİVERSİTESİ KÖTÜCÜL YAZILIMLARDAN KORUNMA POLİTİKASI



| Kodu | Yayınlama Tarihi | Revizyon Tarihi | Revizyon No |
|-----------|------------------|-----------------|-------------|
| BG.PR.001 | 15.04.2026-10/2 | - | - |

1. Amaç ve Kapsam

Bu politikanın amacı, Çankırı Karatekin Üniversitesi'nin bilgi varlıklarını, çalışanlarını ve hizmet verdiği kişilerin verilerini kötücül yazılım tehditlerinden korumak için gerekli prensip ve prosedürleri tanımlamaktır. Bu politika, üniversitenin tüm bilgi teknolojileri varlıklarını, sunucularını, istemcilerini, ağlarını, mobil cihazları ve kullanıcıları kapsar.

2. Tanımlar

- Kötücül Yazılımlar:** Bilgi sistemlerine zarar vermek, verileri çalmak veya sistemleri kullanılamaz hale getirmek amacıyla geliştirilmiş yazılımlar (virüsler, solucanlar, fidye yazılımları, casus yazılımlar, vb.).
- Bilgi Varlıkları:** Üniversitenin sahip olduğu tüm bilgi, yazılım, donanım ve hizmetler.

3. Politika Esasları

3.1. Kötücül Yazılımdan Korunma Yönetimi

- Tüm bilgi sistemlerinde kötücül yazılımlara karşı koruma yazılımları (antivirüs, anti-malware) yüklenmeli ve güncel tutulmalıdır.
- İşletim sistemleri ve uygulama yazılımlarının güncellemeleri düzenli olarak uygulanmalıdır.
- Tüm cihazlarda güvenlik duvarları etkinleştirilmeli ve ağ güvenlik sistemleri kullanılmalıdır.

3.2. Farkındalık ve Kullanıcı Davranışları

- Kullanıcılara, e-posta ekleri, bilinmeyen kaynaklardan indirilen dosyalar ve şüpheli bağlantılara karşı dikkatli olmaları konusunda eğitim verilmelidir.
- Güncel olmayan veya lisanssız yazılımların kullanımı yasaktır.

3.3. Kötücül Yazılım Tarama ve Denetimleri

- Bilgi sistemleri periyodik olarak kötücül yazılım taramasından geçirilmelidir.
- Şüpheli olaylar veya belirtiler fark edildiğinde, bilgi işlemleri birimi derhal bilgilendirilmelidir.

3.4. Olay Yönetimi

- Kötücül yazılım kaynaklı bir olayın tespiti durumunda, olayın etkileri izole edilerek sistemin zararını en aza indirecek önlemler alınmalıdır.
- Tüm olaylar kayıt altına alınmış ve incelenmiş olmalıdır.
- Olayın tekrarlanmasını önlemek için düzeltici eylemler planlanmalı ve



**ÇANKIRI KARATEKİN ÜNİVERSİTESİ
KÖTÜCÜL YAZILIMLARDAN KORUNMA
POLİTİKASI**



| Kodu | Yayınlama Tarihi | Revizyon Tarihi | Revizyon No |
|-----------|------------------|-----------------|-------------|
| BG.PR.001 | 15.04.2026-10/2 | - | - |

uygulanmalıdır.

3.5. Yedekleme ve Kurtarma

- Kritik veriler düzenli olarak yedeklenmeli ve yedekler kötücül yazılım bulaşması riskine karşı izole bir ortamda saklanmalıdır.
- Kötücül yazılım bulaşması durumunda veri kurtarma planı devreye alınmalıdır.

4. Rol ve Sorumluluklar

- **Bilgi ve İletişim Güvenliği Komisyonu:** Politikanın uygulanması ve sürekliliğini sağlamak.
- **Bilgi İşlem Daire Başkanlığı:** Koruma yazılımlarının yüklenmesi, güncellenmesi ve tarama faaliyetlerini yürütmek.
- **Sistem Kullanıcıları ve Son Kullanıcılar:** Politika esaslarına uymak ve şüpheli durumları bildirmek.

5. Yaptırımlar

Bu politikaya uymayan her türlü eylem, yükseköğretim kurumlarını kapsayan ilgili disiplin mevzuatı çerçevesinde değerlendirilir. İhlaller, ilgili mevzuatta belirtilen çeşitli yaptırımlara tabi olabilir.

6. Yürürlük

Bu politika, Çankırı Karatekin Üniversitesi Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.