TÜRK-ALMAN ÜNİVERSİTESİ

ZARARLI YAZILIMLARDAN KORUNMA POLİTİKASI

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

1. AMAÇ

Bu politikanın amacı, Türk-Alman Üniversitesi bilgi sistemlerini zararlı yazılım (malware) tehditlerine karşı korumak, sistemlerin güvenliğini sağlamak ve iş sürekliliğini temin etmektir. Politika, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 3.1.3.2 maddesine dayalı güvenlik tedbirlerine uygunluğu hedeflemektedir.

2. KAPSAM

Bu politika, Türk-Alman Üniversitesi'nin sahip olduğu veya kullandığı tüm bilgi sistemlerini, yazılımları, donanımları, ağları ve çalışanlarını kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından Yönetim Temsilcisi başta olmak üzere tüm personel sorumludur.

4. UYGULAMA

Tanımlar;

Zararlı Yazılım (Malware) : Virüsler, solucanlar, truva atları, fidye yazılımları, istenmeyen reklam yazılımları, casus yazılımlar ve diğer zararlı kodları içeren yazılımlardır.

Anti-Malware Yazılımı : Zararlı yazılımları tespit ve imha etmek için kullanılan araçlar.

Uygulama esasları;

a) Kurumun bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.

b) Düzenli aralıklarla anti-virüs yazılımı otomatik veya manuel olarak güncellenecektir.

c) Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek

d) Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.

e) Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz veya durduramaz. Bunun için gerekli altyapı tesis edilecektir.

f) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

g) Bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir. Bu tür kaynaklardan dosya indirilmesi yasaktır.

h) Bilgisayarlarda kullanılan CD, USB gibi depolama aygıtları virüs taraması yapılmadan kullanılmamalıdır.

i) Kurum dışı CD, USB vb. materyaller kurum bilgisayarlarına takılmamalıdır. Oluşabilecek her türlü olumsuzluklardan personel sorumludur.

j) Kurum ağına anti-virüs programı güncel olmayan bilgisayarlar dâhil edilmemelidir.

k) Bilgi İşlem Daire Başkanlığı tarafından onaylanan yazılımların (Beyaz Listeye alınan yazılımlar) dışında yazılımların bilgi sistemleri altyapısında kullanılması yasaktır. Bilgi İşlem Daire Başkanlığı bu konuda gerekli teknolojik tedbirleri almakla yükümlüdür.

l) Internet üzerinden indirilen her türlü yazılım özet (HASH) bilgisi kontrolü yapıldıktan sonra kullanıma alınmalıdır.