1. **AMAÇ**

Bu talimatın amacı Veri Sorumlusu Süleyman Demirel Üniversitesi ’ne ait kişisel veri içeren bilgi sistemlerini virüslere karşı korumak için ilgili kuralları belirlemektir.

1. **KAPSAM**

Bu talimat Süleyman Demirel Üniversitesi  tarafından kullanılan ve kişisel veri içeren tüm bilgi sistemlerini kapsar.

1. **SORUMLULUKLAR**

İşbu talimatın uygulanmasından tüm çalışanlar sorumludur.

1. **UYGULAMA**
	1. **Anti-Virüs Yazılımı Özellikleri**

Merkezi yönetim yazılımının şu özelliklere sahip olması gerekir:

* Uzaktan kurulum,
* Kullanıcıların yapılan ayarları değiştirmesini, servisleri durdurmasını, programı kaldırmasını önleme kabiliyeti,
* Virüs tanımlarının merkezi olarak güncelleyebilme,
* Periyodik tarama ayarları,
* İsteğe bağlı tarama yapabilme,
* Sürekli (dosya yaratıldığında, kopyalandığında, okunduğunda, değiştirildiğinde vb.) tarama ayarları,
* Antivirüs istemcilerinin statülerinin izlenmesi (bağlantı durumu, antivirüs servisinin durumu,
* Virüs tanımlarının güncelliği, virüs bulundu uyarısı, tarama motorunun ve yazılımın versiyonu bilgisi, IP bilgisi vb.
* Antivirüs yazılımlarının üreteceği kayıtlara erişim,
* Virüs yayılması konularında antivirüs yöneticisini bilgilendirecek e-post, anlık mesaj vb. uyarı mekanizmaları,
* Raporlama özelliği.
	1. **Kurulum**
* Merkezi antivirüs yapısı kurulurken ağ topolojisi ve farklı ağ bölümleri arasındaki hatların hızları dikkate alınmalıdır. Tek merkezi antivirüs yönetim sunucusu kurulumu yerine, farklı ağ bölümlerinde (uzak ofislerde) yardımcı antivirüs sunucuları kurulmalı, bu sunucular merkezi antivirüs yönetim sunucusuna bağlanıp konfigürasyonları virüs tanım dosyalarını, tarama motoru güncellemelerini almalıdır.
* Yoğun antivirüs trafiğinin oluştuğu anlardaki ihtiyaçları karşılamak için gerekli ise merkezi antivirüs sunucusu için İkili/Yedekli bir yapı kurulumu sağlanmalıdır. Mümkün olması durumunda ikili / yedekli yapıda çalışacak sunucular için farklı işletim sistemi kullanımı tercih edilmelidir, böylece iki sunucunun da benzer açıklıklar sonucunda devre dışı kalması önlenecektir.
	1. **Konfigürasyon / Yönetim**

Merkezi antivirüs yapısının kurulum işlemi sonrasında, sunucular ve kullanıcı bilgisayarları üzerlerinde çalışan uygulamalara, maruz kaldıkları tehditlere, zorunlu ise taramalarda kapsam dışı tutulması gereken dosya dizinlere, periyodik taramaların zamanına vb. farklı politika uygulanma ihtiyaçlarına göre gruplandırılmalı ve konfigürasyonları gruplara yapılmalıdır.

* 1. **İmzaların Güncelliği**

Antivirüs yazılımının başarılı olabilmesi için imza güncellemelerinin zamanında yüklenmesi sağlanmalıdır. Tavsiye edilen güncelleme periyodu günlüktür. Fakat bazı acil virüs saldırısı durumlarında daha kısa aralıklarla güncelleme yapılması gerekebilmektedir. İmza güncellemelerine ek olarak antivirüs yazılımları için tarama motoru güncellemeleri ve yamalar da yayınlanmaktadır. Bunların da e-posta listeleri üzerinden takip edilmesi ve istemcilere zamanında ve mümkünse merkezi olarak yüklenmeleri gerekmektedir.

* 1. **Gerçek Zamanlı Virüs Koruma**

Gerçek zamanlı virüs koruma tarama ayarları;

* Dosya Erişim metoduna göre: Seçenekler: Açma, Okuma, Değiştirme, Kopyalama, Hepsi, vb., Tavsiye edilen: Hepsi,
* Dosya Türüne göre: Seçenekler: Çeşitli dosya uzantıları girilebilir, Tavsiye edilen: Hepsi, Taranacak birimler / dizinler: Seçenekler: Ağ bağlantıları, C:\Windows vb., Tavsiye edilen: Hepsi,
* İstisnalar: Tavsiye Edilen: Çeşitli uygulamalar bazı dizinlerin tarama kapsamı dışında tutulmasını gerektiriyor olabilir (Microsoft Exchange vb.), bu tür zorunlu durumlar dışında istisna tanımlanmamalıdır. İstisna tanımlamaları periyodik olarak kontrol edilmelidir.
* Müdahale Yöntemi: Virüs bulunduğunda temizleme, karantinaya alma ya da silme işlemlerinden biri tercih edilmiş olmalıdır
	1. **Periyodik / İsteğe Bağlı Tarama**

Periyodik taramalar için tavsiye edilen periyot kritik bileşenler için günlük, daha az kritik bileşenler için ise haftalıktır. Periyodik tarama zamanı seçilirken, bileşenlerin açık olduğu ve tarama sonucu oluşacak performans kaybının etkisinin en az hissedileceği zamanların seçilmesine dikkat edilmelidir. Tarama işlemlerini kullanıcıların durduramaması sağlanmalıdır.

* 1. **İzleme / Raporlama / Uyarı Ayarları**

Mümkün olan tüm bileşenlere antivirüs yazılımının kurulması ve ayarların yukarıda belirtildiği şekilde yapılması virüslere karşı güvenlik mekanizmasının oluşturulmasını sağlamaktadır. Bileşenlerin durumu uygun şekilde takip edilmezse:

* Antivirüs yazılımı kaldıran / servisi durdurulan / ayarları değiştirilen / antivirüs yazılımı hiç kurulmamış bileşenler fark edilmeyebilir,
* Antivirüs yazılımının temizlemekte başarısız olduğu ya da antivirüs yazılımını etkisiz hale getiren virüsler zamanında fark edilmeyebilir.
* Virüslerin yoğun olarak bulaştığı bileşenler ve bulaşma yöntemleri fark edilemez ve önlem alınamayabilir.
* Virüs tanımları güncel olmayan antivirüs yazılımları belirlenemeyebilir,

Sonuç olarak sistem geciken müdahale sebebiyle zarar görebilir. Bu sebeplerle merkezi antivirüs yazılımı üzerinde bileşenlerin durumları (virüs bulaşmış, virüs tanımı güncel değil, ulaşılamıyor vb.) düzenli olarak kontrol edilmeli, çok sayıda bileşenin olduğu durumlarda raporlama özelliği kullanılarak müdahale gereken bileşenler belirlenmeli, sisteme bulaşan virüsler hakkında detaylı bilgiler alınmalıdır. Ayrıca birçok merkezi antivirüs yazılımında bulunan e-posta ya da anlık mesajla uyarı sistemi devreye sokularak antivirüs sistemi yöneticisinin acil durumlara tepkisi hızlandırılmalıdır.

* 1. **E-Posta Antivirüs Koruması**
		1. **Virüs İmzalarının Güvenliği**

Bölüm 3.1 de yer alan hususlar bu kısımda da geçerlidir.

* + 1. **Virüs Tarama**

E-posta ile bulaşan virüsler çoğunlukla eklenti dosyalarla gelmektedir. Bazı virüsler herhangi bir eklenti olmadan da bulaşabilmektedirler. Virüs tarama ayarları bütün eklenti dosyalar ve e-posta içeriği taranacak şekilde yapılması gerekmektedir. Ayrıca yapılacak ayarla sıkıştırılmış eklenti dosyalarının da taranması sağlanmalıdır. E-posta antivirüs yazılımı seçilirken, yazılımın e-postaları posta kutusuna düşmeden tarama yapma yeteneği olması beklenmektedir. Tarama yapılmamış epostaların sırada bekletilmesi ve tarama sonrasında kullanıcının erişebilmesi sağlanmalıdır. Ek olarak periyodik tarama ile e-posta sunucusunda önceden tespit edilememiş virüslerin temizlenmesi sağlanmalıdır. Örneğin periyodik tarama sıklığı haftalık olabilir.

* + 1. **Eklenti Bloklama Kuralları**

E-posta antivirüs sunumcusu virüs taramasını mevcut virüs imzalarına göre yapmaktadır. Bu çalışma yöntemi dolayısıyla henüz tanımlanmamış virüslerin e-posta yoluyla yayılmaya devam etmesi mümkündür. Bu sebeple virüs içerebilecek dosya türlerinin bloklanması etkin bir önleyici çözüm olarak düşünülmektedir. Bloklanması önerilen uzantılar şunlardır: .asd, .asf, .asx, .bas, .bat, .chm, cmd, .com, .dll, .exe, .hlp, .hta, .hto, .js, .jse, .link, .lnk, .pif, .reg, .scr, .vb, .vbe, .vbs, .wsf, .wsh, ve .wsc. Burada verilen liste virüs taşıyabilecek dosya türlerinin tamamını kapsamayabilir. Antivirüs yöneticileri tecrübelerinden ve BT güvenlik sitelerinde yayınlanan uyarılardan yararlanarak tehdit oluşturabilecek uzantıları bloklama listesine eklemelidir. Ayrıca e-posta eklenti dosyaları yoluyla yayılan bir virüs saldırısı durumunda geçici süreliğine bazı dosya türlerinin bloklanması acil müdahalenin engelleme aşamasında etkin bir çözüm olarak kullanılabilir.

* + 1. **Başlık Bloklama kuralları**

Virüsler e-posta yoluyla yayılırken kullandıkları, dikkat çekme amacı taşıyan başlıklar (Para, seks, iş teklifi vb. kelimeler içeren başlıklar) kullanabilmektedir. E-posta antivirüs yazılımlarında bu tür başlıklarda kullanılan anahtar kelimeleri içeren listeler bulunmaktadır. Antivirüs yöneticisinin mevcut anahtar kelimeleri içeren başlık bloklamayı aktif hale getirmesi, gerekli görüldüğünde listeyi güncellemesi tavsiye edilmektedir.

* + 1. **İzleme / Raporlama / Uyarı Ayarları**

Bir e-posta virüsü, istenmeyen uzantılı eklentili ya da başlığı sebebiyle bloklandığında güvenlik sebebiyle antivirüs yöneticisi için, e-posta kaybının yol açabileceği iş kayıplarını önlemek amacıyla gönderici ve alıcıların bilgilendirilmesi önem taşımaktadır. Dışarıdan gönderilen e-posta mesajlarında ise muhtemel dış saldırganlara bilgi verilmemesi amacıyla göndericiye geri bildirim yapılmaması tercih edilir.