

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı İşletim Sistemi Üzerine Yazılım Kurulumu Ve Güvenliği Prosedürü	Doküman No	PR-028
		İlk Yayın Tarihi	9.9.2022
		Revizyon Tarihi	9.9.2022
		Revizyon No	000
		Sayfa No	1 / 3

1. AMAÇ

Bu prosedürün amacı, **Süleyman Demirel Üniversite Bilgi İşlem Daire Başkanlığının** Bilgi Güvenliği Yönetim Sisteminde işletim güvenliğini sağlayarak bilgi işleme olanaklarının doğru ve güvenli işletimlerini temin ve işletim sistemi üzerine yazılım kurulumunun kontrolü sağlamaktır.

2. KAPSAM

Bu prosedür işletim sistemi üzerine kurulan tüm yazılımları ve bilgi işlem birimlerini kapsamaktadır.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından Bilgi İşlem Hizmetleri Şube Müdürü sorumludur.

4. UYGULAMA

İşletimdeki sistemlerde yazılım değişimi kontrolünde aşağıdaki hususlara dikkat edilmelidir;

- Güncellemeler yetkin sistem yöneticileri Bilgi İşlem departmanı tarafından yapılmalıdır.
- Uygulama ve operasyonel sistem yazılımlarının başarılı test sonrasında uygulanması sağlanmalıdır.
- Konfigürasyon kontrol sistemi (Eski ve yeni yazılım sürümleri, yazılımla ilgili konfigürasyon bilgileri ve sistem dokümantasyonu) uygulanmalıdır.
- Değişiklikler uygulanmadan önce geri dönüş stratejileri oluşturulması ve değişiklikler için log tutulması gerekmektedir.
- Değişiklikleri uygulamadan önce bir geri alma stratejisi uygulanmalıdır.
- Tedarikçiden alınmış yazılımlarda destek alınamaması riskinin göz önüne alınmasıdır.(destek süresi)
- İşletimdeki sistemlerde sadece çalıştırılabilir onaylı kod bulunmalıdır, geliştirme kodu veya derleyiciler olmamalıdır.
- Uygulama yazılımlarının eski sürümleri bir acil durum önlemi olarak saklanmalıdır.
- İşletimsel program kütüphanelerinin tüm güncellemelerinin bir denetim kaydı olmalıdır.
- Yeni bir sürüme yükseltme kararı alındığında değişim için iş gereksinimleri ve sürüm güvenliği dikkate alınmalıdır. Örneğin; yeni bilgi güvenliği işlevleri tanıtımı ya da bu sürümü etkileyen bilgi güvenliği sayısı ve şiddeti hesaba katılmalıdır. Bilgi güvenliği açıklıklarının azaltılmasına ya da kaldırılmasına yardımcı olmak için yazılım yamaları uygulanmalıdır.
- Tedarikçilere fiziksel veya mantıksal erişim gerektiğinde yalnızca destek amacıyla ve yönetimin onayı ile verilmelidir. Tedarikçinin faaliyetleri izlenmelidir.
- Bilgisayar yazılımı, dışardan sağlanan yazılım ve modüllere temel alıyor olsa bile yetkisiz değişiklikleri önlemek için bu yazılım ve modüller güvenlik açıklıkları oluşturabileceğinden izlenmeli ve kontrol edilmelidir.

4.1. İşletim Güvenliği

4.1.1. Yazılı İşletim Prosedürleri

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı İşletim Sistemi Üzerine Yazılım Kurulumu Ve Güvenliği Prosedürü	Doküman No	PR-028
		İlk Yayın Tarihi	9.9.2022
		Revizyon Tarihi	9.9.2022
		Revizyon No	000
		Sayfa No	2 / 3

Bilgi Sistem Altyapısı ile ilgili olarak hazırlanan dokümantasyon Kalite ve Süreç Yönetimi onayından geçip “xxxx” klasörü adı ile ağda yayınlanmaktadır. Politikalar, prosedürler, talimatlar ve takip formları yetkileri dâhilinde kullanıcılar tarafından erişilebilirdir.

4.1.2. Kapasite Yönetimi

Gerekli sistem performansını sağlamak için; izlenen, gelecekteki kapasite gereksinimleri için projeksiyonlar yapılan kaynaklar şunlardır:

CPU, RAM, HDD kapasiteleri izlenir. Bu kapasiteler için ön tanımlı değerleri referans alınır.

Lisanslar tüm şirkette Microsoft sistemlerine ilişkin Sunucu, istemci lisansları Bilgi İşlem Departmanı tarafından takip edilir.

4.1.3. Geliştirme, Test ve İşletim Ortamlarının Ayrımı

Çalışma ortamı ile test ortamı ayrılmıştır Fiziksel test sunucusu ile sanal sunucular oluşturulmaktadır, farklı hizmetler için testler gerçekleştirilmektedir. Testler 3. Taraf hizmet sağlayıcısı tarafından gerçekleştirilmektedir. Bilgi İşlem Departmanına bilgi verilerek canlı ortama alınmaktadır.

4.1.4. Kötücül Yazılımlara Karşı Kontroller

Zararlı kodların sistem sızmalarını engellemek ve sızmaları durumunda temizlemek amacıyla antivirüs yazılımı kullanılmaktadır.

4.2. İşletimsel Yazılımın Kontrolü

4.2.1. İşletimsel Sistemler Üzerine Yazılım Kurulumu

Microsoft lisanslı işletim sistemleri VLSC lisanslamaya tâbi tutulmaktadır. Doğrudan Microsoft'un sitesi üzerinden indirilen lisanslar kullanılarak kurulum gerçekleştirilmektedir.

Açık kaynak kodlu işletim sistemlerinin (Linux, FreeBSD vb.) kurulumu, internet üzerinden indirilen sürümleri kullanılarak gerçekleştirilmektedir.

4.3. Teknik Açıklık Yönetimi

Tespit edilen açıklıklar tanımlanarak teknik çalışan tarafından giderilmektedir.

4.4. Yazılım Kurulumu Kısıtlamaları

Kurum içinde çalışan tarafından kullanılacak sistemlerin kurulumu sırasında, kötü amaçlı yazılımları engelleyici programlar kullanılmaktadır. Bunun dışındaki bütün kısıtlamalar, Group Policy ile sağlanan network ve sistem güvenliği aracılığıyla yapılmaktadır.

5.REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	09.09.2022	İlk yayın.



SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı
İşletim Sistemi Üzerine Yazılım Kurulumu Ve
Güvenliği Prosedürü

Doküman No PR-028

İlk Yayın Tarihi 9.9.2022

Revizyon Tarihi 9.9.2022

Revizyon No 000

Sayfa No 3 / 3
