1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde kullanılan bilgi sistemlerinde işletim sistemi ve işletim sistemi üzerine kurulan yazılımların güvenli, kontrollü ve yetkilendirilmiş şekilde kurulmasını, güncellenmesini, değiştirilmesini ve işletilmesini sağlamaktır.

2. KAPSAM

Bu prosedür, Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde kullanılan sunucu, istemci ve diğer bilgi sistemlerinde işletim sistemi üzerine kurulan yazılımları, yazılım güncellemelerini, yamaları ve işletimsel yazılım değişikliklerini kapsar.

3. TANIMLAR

- ***İşletim Sistemi:*** Bilgisayar donanım ve yazılım kaynaklarını yöneten ve diğer yazılımların çalışmasını sağlayan temel sistem yazılımını,
- ***İşletimsel Yazılım:*** Bilgi sistemlerinin işletilmesi amacıyla kullanılan uygulama, yardımcı program, sistem yazılımı ve benzeri yazılımları,
- ***Yetkili Kullanıcı:*** Bilgi sistemleri üzerinde belirli işlemleri gerçekleştirmek üzere yetkilendirilmiş kullanıcıyı,
- ***Teknik Açıklık:*** Bilgi sistemlerinin güvenliğini olumsuz etkileyebilecek yazılım, donanım, yapılandırma veya uygulama kaynaklı zafiyeti,
- ***Geri Dönüş Stratejisi:*** Yapılan yazılım değişikliği veya güncellemenin başarısız olması durumunda sistemin önceki çalışan durumuna döndürülmesi için belirlenen yöntemi ifade eder.

4. SORUMLULUKLAR

- **Bilgi İşlem Daire Başkanlığı:** İşletim sistemi ve yazılım kurulumları ile güncelleme, yama, güvenlik ve teknik kontrollerin yürütülmesini sağlamak.
- **İlgili Birimler:** Kullanılan yazılımlara ilişkin ihtiyaçları ve iş gereksinimlerini belirlemek, yetkisiz yazılım kullanımını önlemek.
- **Kullanıcılar:** Kendilerine tahsis edilen sistemlere yetkisiz yazılım yüklememek ve belirlenen bilgi güvenliği kurallarına uymak.
- **Tedarikçiler:** Kendilerine verilen yetkiler kapsamında, Üniversitenin bilgi güvenliği kurallarına uygun olarak destek faaliyetlerini gerçekleştirmek.

5. UYGULAMA

5.1. Yazılım Kurulumu ve Değişiklik Yönetimi

İşletim sistemi ve işletim sistemi üzerine kurulacak yazılımların kurulumu, güncellenmesi ve değiştirilmesi yetkili personel tarafından gerçekleştirilir.

Yazılım kurulumu ve değişikliklerinde aşağıdaki hususlar dikkate alınır:

- Yazılım ve güncellemeler güvenilir ve yetkili kaynaklardan temin edilir.
- Kurulumu yapılacak yazılımın lisans durumu, güvenlik gereksinimleri ve sistemle uyumluluğu değerlendirilir.
- Kritik sistemlerde yapılacak değişiklikler öncesinde gerekli yedekleme ve geri dönüş imkânları değerlendirilir.
- Değişikliklerin uygulanması ve sonuçları gerektiğinde kayıt altına alınır.
- Yeni sürüme geçişlerde iş gereksinimleri, sistem uyumluluğu ve bilinen güvenlik açıklıkları dikkate alınır.
- Güvenlik açıklıklarını gidermeye yönelik güncelleme ve yamalar, sistemin hizmet sürekliliğini ve uyumluluğunu etkilemeyecek şekilde uygulanır.
- İşletim ortamlarında yalnızca kullanım için gerekli ve onaylanmış yazılımların bulunması sağlanır.
- Geliştirme araçları, derleyiciler ve benzeri araçlar üretim sistemlerinde ihtiyaç bulunmadıkça bulundurulmaz.
- Kullanılmayan veya destek süresi sona ermiş yazılımlar değerlendirilerek kaldırılır veya gerekli güvenlik önlemleri alınır.
- Yazılımın önceki sürümünün saklanması, geri dönüş ihtiyacı ve sistemin kritikliği dikkate alınarak gerçekleştirilir.

5.2. Yazılım Kaynaklarının ve Lisansların Kontrolü

İşletim sistemi ve yazılımların kurulumunda Üniversite tarafından lisanslanmış veya kullanımına izin verilmiş yazılımlar tercih edilir. Microsoft ürünleri için Üniversitenin sahip olduğu lisanslama modeli kapsamında gerekli lisans kontrolleri Bilgi İşlem Daire Başkanlığı tarafından yürütülür. Açık kaynak kodlu işletim sistemleri ve yazılımlar güvenilir kaynaklardan temin edilir ve kullanılmadan önce sistemin güvenliği ve ihtiyaca uygunluğu değerlendirilir. Kullanılan yazılımların lisans, destek süresi ve üretici tarafından sağlanan güvenlik güncellemeleri gerektiğinde takip edilir.

5.3. Geliştirme, Test ve İşletim Ortamlarının Ayrılması

Geliştirme, test ve işletim ortamlarının birbirinden ayrılması esastır. Yeni yazılım, sürüm veya önemli değişiklikler mümkün olduğu ölçüde test ortamında değerlendirilir. Test sonuçları uygun görüldüğünde ve gerekli kontroller tamamlandığında işletim ortamına aktarılır. Üçüncü taraflar tarafından gerçekleştirilen test veya yazılım çalışmaları, Bilgi İşlem Daire Başkanlığının bilgisi ve ilgili yetkilendirmeler kapsamında yürütülür.

5.4. Konfigürasyon ve Değişiklik Kontrolü

İşletim sistemi ve yazılımlara ilişkin önemli konfigürasyon değişiklikleri kontrollü şekilde gerçekleştirilir.

Değişikliklerde;

- mevcut ve yeni sürüm bilgilerinin,
- gerekli konfigürasyon bilgilerinin,
- değişikliğin nedeninin,
- değişiklik tarihinin,
- değişikliği gerçekleştiren yetkili personelin kayıt altına alınması gerektiğinde sağlanır.

Değişiklik öncesinde sistemin kritikliği ve değişikliğin etkisine göre yedekleme ve geri dönüş yöntemi belirlenir.

5.5. İşletim Güvenliği

Bilgi sistemlerinin güvenli işletimi için gerekli işletim prosedürleri, talimatlar ve diğer dokümanlar Üniversitenin doküman yönetim sistemi üzerinden yayımlanır ve yetkili kullanıcıların erişimine sunulur. İşletim sistemleri ve yazılımların çalışması için gerekli sistem kaynakları izlenir. Özellikle CPU, RAM ve depolama kapasitesi gibi kaynakların kullanım durumu ve ihtiyaçları takip edilir. Kapasite yetersizliği oluşturabilecek durumlarda gerekli teknik değerlendirme ve planlama yapılır.

5.6. Kötücül Yazılımlara Karşı Koruma

Bilgi sistemlerinde kötücül yazılımlara karşı Üniversite tarafından belirlenen güvenlik yazılımları ve teknik kontroller kullanılır. Kötücül yazılım tespiti, şüpheli dosya veya olaylarda ilgili güvenlik ve olay yönetimi süreçleri uygulanır.

5.7. İşletim Sistemleri Üzerine Yazılım Kurulumu

İşletim sistemi üzerine yazılım kurulumu yalnızca yetkilendirilmiş kullanıcılar veya Bilgi İşlem Daire Başkanlığı tarafından belirlenen yetkili personel tarafından gerçekleştirilir.

Kurulum öncesinde;

- yazılımın kaynağı,
- lisans durumu,
- güvenlik durumu,
- işletim sistemiyle uyumluluğu,
- sistem üzerindeki etkisi değerlendirilir.

Kullanıcıların yetkisiz yazılım yüklemesini önlemek amacıyla gerekli işletim sistemi, ağ ve güvenlik kontrolleri uygulanır.

5.8. Teknik Açıklıkların Yönetimi

İşletim sistemi ve yazılımlarda tespit edilen teknik açıklıklar değerlendirilerek gerekli güncelleme, yama, konfigürasyon değişikliği veya diğer teknik kontroller uygulanır. Açıklığın giderilmesinde sistemin kritiklik seviyesi, açıklığın etkisi, üretici güncellemeleri ve hizmet

sürekliliği dikkate alınır. Kritik güvenlik açıklıkları için gerekli durumlarda öncelikli müdahale gerçekleştirilir.

5.9. Tedarikçi Erişimi

Tedarikçilerin bilgi sistemlerine fiziksel veya mantıksal erişimi yalnızca ihtiyaç duyulan hizmetin gerçekleştirilmesi amacıyla, yetkilendirme ve Üniversitenin bilgi güvenliği kuralları kapsamında sağlanır. Tedarikçi erişimleri gerektiğinde süre, kapsam ve yetki bakımından sınırlandırılır ve gerçekleştirilen faaliyetler izlenebilir şekilde kayıt altına alınır. Tedarikçi desteğinin sona ermesi veya erişim ihtiyacının ortadan kalkması durumunda ilgili erişimler kaldırılır.

5.10. Yazılım ve Modüllerin Kontrolü

İşletim sistemleri üzerinde kullanılan üçüncü taraf yazılım, kütüphane, modül ve bileşenler güvenlik ve uyumluluk açısından gerektiğinde değerlendirilir. Güvenlik riski oluşturan, desteklenmeyen veya kullanılmayan yazılım ve bileşenler için kaldırma, güncelleme veya alternatif kontrol uygulanır.

6. İLGİLİ DOKÜMANLAR

- Yazılım ve Bilgi Alışverişi Politikası
- Olay ve İhlal Yönetimi Prosedürü
- Kötücül Yazılımlara Karşı Koruma Politikası
- Bilgi Güvenliği Politikası

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	09.09.2022	İlk yayın.
001	22.01.2024	Kontrol kısmı güncellenmiştir.
002	16.09.2026	SDÜ EYS yapısına uyum sağlanması, kapsam, tanımlar, sorumluluklar ve uygulama hükümlerinin güncellenmesi; yazılım kurulumu, değişiklik, teknik açıklık, işletim güvenliği ve tedarikçi erişimi süreçlerinin yeniden düzenlenmesi.