1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi teknolojileri varlıklarının güvenli yapılandırmalarının belirlenmesi, uygulanması, dokümante edilmesi, izlenmesi ve düzenli olarak gözden geçirilmesini sağlayarak bilgi güvenliğinin korunmasını sağlamaktır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde Üniversitenin kontrolünde bulunan ve bilgi işleme faaliyetlerinde kullanılan;

- Sunucu, istemci, mobil cihaz ve ağ cihazlarını,
- İşletim sistemleri ve uygulama yazılımlarını,
- Bulut hizmetlerini,
- Güvenlik cihazlarını (firewall, router, switch vb.),
- Sanallaştırma ve yedekleme altyapılarını kapsar.

3. SORUMLULAR

- **Bilgi İşlem Daire Başkanlığı:** Güvenli konfigürasyonların belirlenmesi, uygulanması, izlenmesi ve güncellenmesini sağlamak.
- **Varlık Sahipleri:** Sorumlu oldukları varlıkların belirlenen güvenli konfigürasyonlara uygun kullanılmasını sağlamak.
- **Kullanıcılar:** Kendilerine tahsis edilen cihaz ve sistemlerde belirlenen güvenlik kurallarına uymak.

4. TANIMLAR

- ***Konfigürasyon (Yapılandırma):*** Bir donanım, yazılım, sistem veya ağ bileşeninin çalışma ve güvenlik özelliklerini belirleyen teknik ayarların bütününü ifade eder.
- ***Referans Konfigürasyon (Baseline):*** Bir bilgi teknolojisi varlığı için uygulanması gereken asgari güvenlik ve teknik yapılandırma ayarlarını ifade eder.

5. UYGULAMA

5.1. Konfigürasyonların Belirlenmesi

- Bilgi teknolojileri varlıklarının türüne, kullanım amacına ve risk seviyesine uygun güvenli konfigürasyonlar belirlenir.
- Gerekli görülen varlık türleri için referans konfigürasyonlar (baseline) oluşturulur.
- Yeni kurulan veya hizmete alınan sistemler, mümkün olduğu ölçüde belirlenen referans konfigürasyonlara uygun şekilde yapılandırılır.

5.2. Güvenli Konfigürasyon Esasları

Konfigürasyonlar oluşturulurken aşağıdaki güvenlik esasları dikkate alınır:

a) Sunucu ve İşletim Sistemleri

- Kullanılmayan servis ve özellikler devre dışı bırakılır.
- Varsayılan hesap ve parolalar değiştirilir veya gerekli değilse devre dışı bırakılır.
- Yetkiler görev ve sorumluluklara uygun olarak sınırlandırılır.
- Güvenlik güncellemeleri ve yamalar uygulanır.
- Gerekli sistem ve güvenlik loglarının tutulması sağlanır.

b) Ağ ve Güvenlik Cihazları

- Varsayılan parolalar değiştirilir.
- Yönetim erişimlerinde güvenli protokoller kullanılır.
- Gereksiz port, servis ve protokoller kapatılır.
- Ağ erişim kuralları yetkilendirme ve güvenlik gereksinimlerine göre yapılandırılır.
- Konfigürasyon yedekleri güvenli şekilde saklanır.

c) Uygulamalar

- Varsayılan hesap ve ayarlar güvenlik gereksinimlerine uygun şekilde değiştirilir veya devre dışı bırakılır.
- Gereksiz özellik ve eklentiler kullanılmaz.
- Kullanıcı erişimleri görev ve sorumluluklara uygun olarak tanımlanır.
- Gerekli uygulama ve güvenlik loglarının tutulması sağlanır.

ç) Bulut Hizmetleri

- Yönetici hesaplarında, hizmetin desteklemesi ve risk seviyesinin gerektirmesi halinde çok faktörlü kimlik doğrulama (MFA) kullanılır.
- Erişim yetkileri en az ayrıcalık prensibine göre belirlenir.
- Veri güvenliği için hizmetin sunduğu uygun şifreleme ve güvenlik mekanizmaları kullanılır.
- Erişim ve güvenlik kayıtları, hizmetin niteliğine ve risk seviyesine uygun olarak izlenir.

5.3. Konfigürasyonların Dokümantasyonu

- Konfigürasyon değişiklikleri ve gerekli konfigürasyon bilgileri Konfigürasyon Kayıt Formu veya kullanılan uygun kayıt yöntemi ile dokümante edilir.
- Konfigürasyon dosyaları ve yedekleri yetkisiz erişime karşı korunur.
- Konfigürasyon kayıtlarının güncel tutulması sağlanır.

5.4. Konfigürasyon Değişiklikleri

- Konfigürasyonlarda yapılacak değişiklikler Değişiklik Yönetimi Prosedürü doğrultusunda gerçekleştirilir.

- Değişikliklerin güvenlik ve hizmet sürekliliği üzerindeki etkileri gerekli durumlarda değerlendirilir.
- Onaylanan değişiklikler uygulanır ve değişiklik sonrası konfigürasyon kayıtları güncellenir.

5.5. İzleme ve Kontrol

- Konfigürasyonların belirlenen güvenlik gereksinimlerine uygunluğu, sistemin niteliği ve risk seviyesine göre uygun teknik yöntemlerle izlenir.
- Yetkisiz veya uygunsuz konfigürasyon değişiklikleri tespit edildiğinde gerekli düzeltici işlemler gerçekleştirilir.
- Konfigürasyon uygunsuzlukları ve güvenlik olayları ilgili süreçler kapsamında değerlendirilir.

5.6. Gözden Geçirme

- Referans konfigürasyonlar ve güvenlik ayarları en az yılda bir kez veya aşağıdaki durumlarda gözden geçirilir:
  - Önemli sistem veya teknoloji değişikliklerinde,
  - Güvenlik zafiyeti veya güvenlik olayı meydana geldiğinde,
  - Mevzuat veya güvenlik gereksinimlerinde değişiklik olduğunda,
  - Yeni tehdit veya risklerin ortaya çıkması durumunda.

- Gözden geçirme sonucunda gerekli görülen konfigürasyon güncellemeleri ve iyileştirmeler gerçekleştirilir.

6. İLGİLİ DOKÜMANLAR

- Konfigürasyon Kayıt Formu
- Değişiklik Yönetimi Prosedürü

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	29.09.2025	İlk yayın.
001	16.09.2026	SDÜ EYS yapısına uyum sağlanması, kapsam ve sorumlulukların güncellenmesi, güvenli konfigürasyon, değişiklik, izleme ve gözden geçirme süreçlerinin yeniden düzenlenmesi.