1. AMAÇ

Bu politikanın amacı Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı'nın sahip olduğu sunucularının temel güvenlik yapılandırmaları için standartları belirlemektir.

2. KAPSAM

Bu politika Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı'nın sahip olduğu tüm sunucuları ve sunucuların sistem yöneticilerini kapsamaktadır.

3. SORUMLULUK

Bilgi İşlem Daire Başkanlığı bünyesindeki bütün dahili sunucuların yönetiminden, yetkilendirilmiş sistem yöneticileri sorumludur.

4. UYGULAMA

- Sunucu kurulumları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
- Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
- Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
- Servislere erişimler sistem yöneticileri tarafından 6 (altı) ay boyunca loglanacak ve erişim kontrol metotlarıyla koruma sağlanacaktır.
- Sunucular üzerinde yapılacak değişiklikler yönetim kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

- Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdırlar. Gerekli olduğunda, önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
- Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda (sistem odalarında) bulundurulmalıdır.
- Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.
- Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.
- Port tarama atakları düzenli olarak yapılmalıdır.
- Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
- Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.