|  |  |  |  |
| --- | --- | --- | --- |
|  | **POLİTİKALAR** | **Doküman No:** | BT-PO-0008 |
| **Yayın Tarihi:** | 08.06.2022 |
| **Değişiklik No:** | 0 |
| **Değişiklik Tarihi:** | ­- |

**ANTALYA BİLİM ÜNİVERSİTESİ**

**BİLGİ İŞLEM MÜDÜRLÜĞÜ**

**SUNUCU GÜVENLİK POLİTİKASI**

# AMAÇ

Bu politikanın amacı Antalya Bilim Üniversitesi Bilgi İşlem Müdürlüğü’nün sahip olduğu sunucularının temel güvenlik yapılandırmaları için standartları belirlemektir. Bu politikanın etkili uygulanmasıyla Antalya Bilim Üniversitesi bünyesinde bulunan sunuculara ve teknolojiye yetkisiz erişimler minimalize edilecektir.

# KAPSAM

Sunucu Güvenlik Politikası, Antalya Bilim Üniversitesi Bilgi İşlem Müdürlüğü’nün sahip olduğu tüm sunucuları ve sunucuların sistem yöneticilerini kapsamaktadır.

# SORUMLULUK

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

# UYGULAMA

1. Sunucu kurulumları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır.
2. Üniversitede bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel sorumludur.
3. Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
4. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
5. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
6. Servislere erişim logları sistem yöneticileri tarafından 5 (beş) yıl boyunca saklanacak ve erişim kontrol metotlarıyla koruma sağlanacaktır.
7. Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN’larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
8. 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.
9. Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda (sistem odalarında) bulundurulmalıdır.
10. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir
11. Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.
12. Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.
13. Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
14. Sunucuların yazılım ve donanım bakımları Bilgi İşlem Müdürlüğü’nün belirlediği aralıklarla, yetkili personel tarafından yapılmalıdır.
15. Sunucular üzerinde yapılacak değişiklikler yönetim kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.