1. AMAÇ:

Bu politikanın amacı İstanbul Üniversitesi'nin sahip olduğu sunucularının temel güvenlik yapılandırmaları için standartları belirlemektir. Bu politikanın etkili uygulanmasıyla, İstanbul Üniversitesi bünyesindeki sunuculara ve teknolojiye yetkisiz erişimler en alt düzeye indirgenecektir.

2. KAPSAM:

Bu politika İstanbul Üniversitesi'nin sahip olduğu tüm sunucuları ve sunucuların sistem yöneticilerini kapsamaktadır.

3. SORUMLULAR:

Kurum bünyesindeki bütün dahili sunucuların yönetiminden, yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu yapılandırmaları sadece bu gruptaki kişiler tarafından yapılacaktır.

4. KURALLAR:

- Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
- Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır.
- Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
- Sunucu olarak kullanılmak istenen makineler ve kullanıcıları hakkında bilgiler "***Sunucu Yönetim Talep Formu***" ile resmi yazının ekinde BİDB na iletilmelidir.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- 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.

- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- 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 ve altyapı elemanlarının bulunduğu sistem odalarının bakım ve kontrolünde uyulması gereken kurallar ***"Sistem Odaları Kullanım ve Bakım Talimatnamesi"*** içerisinde belirtilmiştir.
- Sunuculara ait bağlantılar normal kullanıcı hatlarına asla takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
- Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.
- Sunucular kasti veya bir ele geçirme (hack) sonucu başka bir sisteme erişme ve zarar verme benzeri girişimler için kullanılmamalıdır. Bu duruma uymayan sunuculara erişim anında kapatılacaktır.
- Sunucular üzerinde kesinlikle ticari amaç güden yazılımlar kurulmamalıdır.
- Sunucular üzerinde daha önce belirtilen servisler haricinde (dosya paylaşımı vb.) başka bir servis çalıştırılmamalıdır.
- Bu politikanın içeriği BİDB web adresinde yayınlandığı tarihten itibaren bütün sunucular için geçerli olacaktır.

5. GÖZLEMLEME

- Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır.
- Bütün güvenlikle ilgili loglara online olarak minimum 180 gün süreyle erişilebilmelidir.
- Loglar sunucu üzerinde tutulmalarının yanında ayrı bir sunucuda daha tutulmalıdır.
- Yedekleme ilgili talimatlar ***"Sunucu Yedekleme Talimatı"*** dökümanında ayrıntılı olarak belirtilmiştir.

- 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.

6. YAPTIRIMLAR

- Kampüs dışına servis sunacak sunucuların güvenlik kontrolleri sunucuyu yöneten sistem sorumluları tarafından yapılmalıdır. Güvenli bulunmayan sunucular BİDB Sistem Yönetim Birimi tarafından tespit edildiğinde sistem sorumlusu bilgilendirilecektir. Buna rağmen gerekli önlemler alınmaz ise sunucunun yerel ağ ve internet erişimi BİDB Sistem Yönetim Birimi tarafından engellenecektir.

7. İLGİLİ DOKÜMANLAR:

1. Bilgi Güvenliği Politikası
2. Sunucu Yedekleme Talimatı
3. Sistem Odaları Kullanım ve Bakım Talimatnamesi
4. Sunucu Yönetim Talep Formu