P11 SUNUCU GÜVENLİK POLİTİKASI

1.1 Amaç

Bu politikanın amacı kurumun sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili kullanılması ile Kurum bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler engellenmesi amaçlanmaktadır.

1.2 Kapsam

Bu politika kurumun sahip olduğu bütün dahili sunucular için geçerlidir.

1.3 Politika

Sunucu Güvenlik politikalar aşağıdaki gibi iki başlıkta ele alınmıştır.

1.3.1 Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sadece Bilgi İşlem sorumludur. Sunucu konfigürasyonları sadece bu Bilgi İşlem tarafından veya onaylı danışmanlık kurumları tarafından Bilgi İşlem gözetiminde yapılacaktır.

a) Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıtlı olmalıdır.
b) Sunucuların Yeri ve Sorumlu Departmanları,
c) Seri Numarası, Marka ve Model Bilgileri,
ç) Donanım Özellikleri,
d) Bakım Bilgisi,
e) Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

1.3.2 Genel Konfigürasyon Kuralları

f) İşletim sistemi yönetimi kurumun Bilgi İşlem Daire Bakanlığı talimatlarına göre yapılmalıdır.
g) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
ğ) En az 1 hafta süreyle loglanmalıdır. (IP bazlı)
h) Kurum dışı yapılan bağlantılar bilgi sistemlerinin belirlediği kurallara göre yapılmalıdır.
ı) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

1.4 Gözlemleme

a) Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalı ve yasalarla belirlenmiş süreler kadar saklanmalıdır.

b) Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
c) Denetimler yetkili organizasyonlar tarafından kurum bünyesinde belli aralıklarda yapılmalıdır.
ç) Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilmelidir.
d) Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
e) Sunucuların yazılım ve donanım bakımları periyodik olarak sistem yöneticileri tarafından yapılmalıdır.
f) Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve loglanmalıdır.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		