



SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı

PERSONEL GÜVENLİK POLİTİKASI

Doküman No	PLT-033
İlk Yayın Tarihi	22.01.2020
Revizyon Tarihi	22.01.2020
Revizyon No	000
Sayfa No	1 / 1

1. AMAÇ

Kurumun bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle kurum, ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten atılması, eğitilmesi, vb. konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

2. KAPSAM

Personel Güvenlik Politikası, Kurum bilgi sistemlerini kullanan tüm çalışanlarını kapsamaktadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından, Süleyman Demirel Üniversitesinde kullanılan otomasyon yazılımlarının ilgili olduğu birimlerin yöneticileri ve Bilgi İşlem Daire Başkanlığı sorumludur.

4. UYGULAMA

a. Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

b. Kullanıcılara erişim haklarını açıklayan yazılı bildirimler verilmeli ve teyit alınmalıdır.

c. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

ç. Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.

d. Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

e. Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.

f. Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

g. Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.

ğ. Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.

h. İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.

ı. Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

i. Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

Hazırlayan	Kontrol	Onay
Merve GÜNEŞ	Gözde BİÇEN	Dr. Veli ÇAPALI