P02 PERSONEL GÜVENLİĞİ POLİTİKASI

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 çıkması, eğitilmesi, vb. konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

1.2 Kapsam

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

1.3 Politika

Personel Güvenliği Politikaları aşağıdaki gibidir.

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
b) Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaklanmalıdır.
c) 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.
ç) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
d) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
e) Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
f) Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
g) İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları düzenlenmeli ya da pasife alınmalıdır.
ğ) 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.
h) Yetkiler "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı " rollerin sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla

yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.

ı) Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir.

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

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