



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
PDH.BG.PO.07			--	

## 1. AMAÇ

T.C. Sağlık Bakanlığı Kocaeli İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri bünyesinde Sosyal Mühendislik Zafiyetleri ve Sosyal Medya Güvenliği konularının nasıl yönetileceğini belirler.

## 2. KAPSAM

Kocaeli İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde ki bütün çalışanları kapsar.

## 3. SOSYAL MÜHENDİSLİK ZAFİYETLERİ POLİTİKASI

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaafalarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

- 1) Taşındığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- 2) Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
- 3) Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
- 4) Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
- 5) Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
- 6) Oluşturulan dosyaya erişecek kişiler ve hakları “bilmesi gereken” prensibine göre belirlenmelidir.



Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
PDH.BG.PO.07			--	

- 7) Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
- 8) Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
- 9) Kaza, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.
- 10) Sadece yetkili kişilerin kurum içerisindeki sınırlı bölümlere erişim izni olduğundan emin olmak için uygun erişim kontrol mekanizmaları olması gerekir.
- 11) İnternette kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve bu sürekli izlenmelidir.
- 12) 'Bilmesi Gerektiği Kadar' prensibine göre hareket edilmelidir.

#### **4. SOSYAL MEDYA GÜVENLİĞİ**

- 1) Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
- 2) Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- 3) Kuruma ait hiçbir gizli bilgi, yazı, sosyal medyada paylaşılmamalıdır.