



**1.AMAC:** Personelin sosyal mühendislik saldırılarından korunması için kişisel olarak dikkat etmesi gereken hususları tanımlamaktır.

**2.KAPSAM:** Personelin sosyal mühendislik saldırılarından korunması için kişisel olarak dikkat etmesi gereken hususları kapsar.

**3.KISALTMALAR:**

**BGYS:** Bilgi Güvenliği Yönetim Sistemi

**EBYS:** Elektronik Belge Yönetim Sistemi

**ÇKYS:** Çekirdek Kaynak Yönetim Sistemi

**4.TANIMLAR:**

**Sosyal Mühendislik:** Normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır.

**5.SORUMLULAR:**

Hatay İl Sağlık Müdürlüğünde faaliyet gösteren tüm personel sorumludur, bu sürecin işletilmesinden ise BGYS Komisyonu ve Hatay İl Sağlık Müdürlüğü makamı sorumludur.

**6.FAALİYET AKIŞI:**

**6.1.** Taşındığımız ve işlediğimiz verilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.

**6.2.** Arkadaşlarımızla paylaştığımız bilgileri seçerken dikkat edilmelidir.

**6.3.** Çöpe atılan kâğıtlara dikkat edilmelidir. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırma makinesinde imha edilmelidir.

**6.4.** Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgiler paylaşılmamalıdır.

**6.5.** Şifre kişiye özel bir bilgidir. Sistem yöneticisi dâhil telefonda veya e-posta ile şifreler paylaşılmamalıdır.

**6.6.** Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.

**6.7.** Oluşturulan dosyaya erişebilecek kişiler ve hakları “bilmesi gereken” prensibine göre belirlenmelidir.

**6.8.** Erişebilecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.

**6.9.** Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.

**6.10.** Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli yetkiler verilmelidir.

**6.11.** Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.

**6.12.** Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.

**6.13.** Hasta mahremiyetine ters düşecek bilgiler paylaşılmamalıdır.

**6.14.** Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz.

**7.İLGİLİ DOKÜMANLAR:**

