T.C.
DENİZLİ VALİLİĞİ
İL SAĞLIK MÜDÜRLÜĞÜ
SOSYAL MEDYA VE SOSYAL MÜHENDİSLİK SALDIRILARINDAN KORUNMA POLİTİKASI

1. AMAÇ

Müdürlüğümüz ve Bağlı Sağlık Tesisleri bünyesinde çalışan personellerin Sosyal Medya ve Sosyal Mühendislik Saldırıları sonucunda oluşabilecek bilgi güvenliği açıklarını engellemek

2. KAPSAM

Denizli İl Sağlık Müdürlüğü Bilgi Güvenliği Yönetim Sistemi Politika metninde yer alan kapsam maddesinde belirlenmiş olan kapsamdır.

3. TANIMLAR

İSM: Denizli İl Sağlık Müdürlüğü
KVKK: Kişisel Verileri Koruma Kurumu

4. SORUMLULUKLAR

Bu prosedürün uygulanmasından ilgili kurum yöneticileri sorumludur.

5. UYGULAMA

5.1. Sosyal Mühendislik Ve Sosyal Medya Güvenliği

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

5.1.1. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

5.1.1.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.

5.1.1.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.

5.1.1.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

5.1.1.4. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız.

5.1.1.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.

5.1.1.6. Oluşturulan dosyaya erişecek kişiler ve haklarını, “bilmesi gereken” prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.

5.1.1.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

5.1.1.8. Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinde imha ediniz.

5.1.1.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.

5.1.1.10. Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.

Hazırlayanlar	Kontrol Eden	Onaylayan

5.1.1.11. Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

5.1.2. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler şu şekilde sıralanabilir:

5.1.2.1. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.

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

5.1.2.3. Hasta dosyaları ilgili doktor ve hemşire dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.

5.1.2.4. Sağlık Bilgi Yönetim Sistemi (SBYS) programlarında kullanılan parolalar kimseyle paylaşılmaz.

5.1.3. Kişisel Sosyal Medya Güvenliği

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

5.1.3.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

5.1.3.3. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

5.1.3.4. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

5.1.3.5. Mobil uygulamalar(WhatsApp, Messenger, Line Viber Skype vb.) ve sosyal medya platformları (Facebook, Youtube, Instagram, Twitter vb.) üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmaz.

6. YAPTIRIM

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayanlar	Kontrol Eden	Onaylayan