

KLVZ-EK-17 BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ

1. AMAÇ:

Bilgi Güvenliği Farkındalık Bildirgesi, T.C. Sağlık Bakanlığı bünyesinde görev yapan kamu çalışanlarının, hizmetin yapılması esnasında veya herhangi bir şekilde öğrendikleri kuruma ait gizli kalması gereken bilgilerin, usulüne uygun olarak korunması için kişisel olarak uymakla sorumlu oldukları bilgi güvenliği kurallarını tanımlar.

2. KAPSAM:

Bu bildirge, Bakanlık bünyesinde görev yapan kamu çalışanlarını bilgilendirmek amacıyla hazırlanmıştır. Kuruma ait gizli kalması gereken bilgileri işleyen diğer personel (danışmanlar, yükleniciler vb.) için Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu ekinde yer alan "Personel Gizlilik Sözleşmesi" hükümleri uygulanır.

3. YASAL DAYANAK:

Bu bildirge, 657 Sayılı Devlet Memurları Kanunu'nun Gizli Bilgileri açıklama yasağı başlıklı 31'nci maddesine, Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018 sayılı Kararı'nın 2'nci maddesinin b fıkrasına, 02/05/2018 tarihli Sağlık Bakanlığı Bilgi Güvenliği Yönergesi'ne ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu'nun 10.5'nci maddesine istinaden hazırlanmıştır.

4. TANIMLAR:

Bu bildirgede geçen;

4.1 Kurum: T.C. Sağlık Bakanlığını (merkez teşkilatı, bağlı kurum ve kuruluşlar ve genel müdürlükler ile bunlara bağlı tüm taşra teşkilatı ve birimleri),

4.2 Kuruma Ait Gizli Kalması Gereken Bilgiler:

4.1.1 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belgeyi,

4.1.2 Kurum tarafından işlenen (24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (21/06/2019 tarihli ve 30888 sayılı Kişisel Sağlık Verileri Hakkında Yönetmelik ile tanımlanan) kişisel sağlık verilerini,

4.1.3 Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belgeyi,

4.1.4 Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işleri ifade eder.

5. PERSONELİN YÜKÜMLÜLÜKLERİ:

5.1 Kuruma ait gizli kalması gereken bilgiler, yasal zorunluluklar ve kurum tarafından resmi olarak izin verilmesi halleri dışında, ilgili mevzuatta belirtilen önlemler alınmak suretiyle koruma altında tutulur. Kurum tarafından aksi belirtilmedikçe, söz konusu bilgiler yasal işleme amaçları haricinde doğrudan veya dolaylı olarak kullanılamaz, başka kişi veya kurumlara aktarılamaz, yayımlanamaz, açıklanamaz veya kişisel kopyaları alınamaz.

5.2 Kuruma ait gizli kalması gereken her türlü bilgi, sır olarak saklanır. Çalışanlar bunları sır olarak saklamak, üçüncü kişilere inceletmemek, söylememek, iletmemek ve açıklamamakla yükümlüdür. Bu yükümlülük, çalışanların Kurum ile ilişkisi sona erse de devam eder.

5.3 Kurumsal ve kişisel sosyal medya hesapları kullanılırken, görevin gerektirdiği dikkat ve özen gösterilir. Kuruma ait gizli kalması gereken bilgiler, hastalara ilişkin kişisel bilgiler (hasta görüntüleri dâhil) hiçbir şekilde sosyal medya ortamlarında paylaşılmaz.

5.4 Kurum tarafından uygun görülen sistemler, uygulamalar, kullanıcı işlemleri ve bilgi sistem ağındaki verilerin ve veri akışının iz kayıtları; hukuki ve idari süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabilir.

5.5 Çalışanlara tahsis edilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazlar, sadece göreve yönelik ve kurumsal faaliyetler için kullanılır.

5.6 Çalışanlara tahsis edilen "kullanıcı adı" ve "parola"lar hiçbir şekilde üçüncü kişiler ile paylaşılmaz. Çalışanlar, kurumdan ayrılmaları halinde kendilerine tahsis edilen kullanıcı adı ve parolaları iptal ettirmekle; kullandıkları bilgisayar ve/veya diğer elektronik veri depolama cihazlarında oluşturduğu veri, bilgi ve belgeler dâhil tüm dosyaları, cihazları ve ofis malzemelerini eksiksiz olarak kurum yetkilisine teslim etmekle ve bunların kopyalarını almamakla yükümlüdür.

5.7 Çalışanlar, bilgisayarlarını kendilerine tahsis edilen "kullanıcı adı" ve "parola" ile oturum açmak suretiyle kullanır. Çalışma sona erince ilgili oturum veya bilgisayar kapatılarak, üçüncü kişilerin bilgisayardaki bilgilere erişimi engellenir. Bilhassa güvensiz ortamlarda, kurum bilgisayarlarının fiziki güvenliği için azami çaba sarf edilir.

5.8 Kurum tarafından sağlanan İnternet üzerinden girilen ve girilemeyen tüm siteler ve adresler, bu maksatla oluşturulan kayıt sistemi tarafından (gerekli olduğunda kullanılmak üzere) otomatik olarak kayıt altına alınır. Çalışanlara tahsis edilen kullanıcı adı ve parola kullanılmak suretiyle usulüne uygun olarak kayıt altına alınan işlemlerden, kullanıcı adı tahsis edilen kişi yasal olarak sorumlu tutulur.

5.9 Çalışanlar, kendilerine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP/MAC adresini kullanılarak gerçekleştirilen her türlü etkinlikten kişisel olarak sorumludur. Aynı şekilde kurum bilişim kaynakları kullanılarak oluşturulan ve/veya tahsis edilen bilişim kaynağı üzerinde bulundurulmuş her türlü bilgi, belge, doküman, yazılım vb. içeriğinden ilgili kişi şahsen sorumludur.

5.10 Çalışanlar, kendilerine teslim edilen kullanıcı adı ve parolanın gizli kalmasını sağlamakla yükümlüdür. Çalışanların şahsi kusurları nedeniyle kullanıcı adı ve parolalarının üçüncü kişiler tarafından öğrenilmesi halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden, kusuru bulunan kişi şahsen sorumlu tutulabilir.

5.11 Çalışanlara tahsis edilen *@sağlık.gov.tr uzantılı tüzel ve kurumsal e-posta hesapları, sadece görevle ilgili faaliyetler için kullanılır. Kurum içinde veya dışındaki kişilere iş ile ilgili olmayan toplu ve/veya kişisel e-posta gönderilmez. Çalışanlar, kurum içine veya kurum dışına göndermiş oldukları tüm e-postalardan kişisel olarak sorumludur.

5.12 Çalışanlar, kendilerine teslim edilmiş yazılım, donanım, araç ve gereç üzerinde; kurum bilgisi dışında mekanik (donanım ekleme, kaldırma vb.) ya da yazılımsal değişiklik (yeni yazılım yükleme, kurum tarafından koyulan bir kısıtlamayı aşmak üzere bilgisayar ayarlarını değiştirme vb.) yapamaz.

5.13 Çalışanlar, kurum tarafından yüklenen işletim sistemi ve uygulama yazılımları haricinde, ilgili birimlerin bilgisi dışında başka yazılımları yükleyemez. Kurum tarafından yüklenmemiş yazılımlardan doğacak sorumluluk, ilgili bilgisayarın sahibi olan kişiye aittir.