# DİYARBAKIR İL SAĞLIK MÜDÜRLÜĞÜ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI

## 1. AMAÇ

Bu politika; Diyarbakır İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde kullanılan bilgi varlıklarının gizliliği, bütünlüğü ve sadece yetki verilen kişilerce erişilebilirliğini sağlayarak, kurum bünyesinde çalışanların ve diğer ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek amacıyla hazırlanmıştır.

## 2. KAPSAM

Bu politika; Diyarbakır İl Sağlık Müdürlüğü hizmet sunumu sürecinde yer alan tüm bilgi sistemlerini, bilişim kaynaklarını, fiziksel bilgi varlıklarını, bilişim ağları ve altyapısını, uygulama yazılımlarını, veri tabanı sistemlerini, tüm bilgi işlenen platform ve süreçleri ve bu süreçlerde görev yapan personel ve tedarikçiler de dâhil tüm paydaşları kapsar.

## 3. DAYANAK

- 21/06/2019 tarihli ve 30808 sayılı Resmi Gazetede yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik (Yönetmelik)
- 02/05/2018 tarihli ve 98813799.719.54 sayılı Bakanlık Makam onayı ile yürürlüğe giren Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi (Yönerge)
- Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu (Sürüm 2.1) (Kılavuz)
- Sağlık Bakanlığı Kurumsal SOME Kurulum ve Yönetim Rehberi (Rehber)
- Cumhurbaşkanlığı tarafından yayımlanan 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" hakkında genelge.

## 4. TANIMLAR ve KISALTMALAR

- **Bilgi Güvenliği:** Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümüdür.
- **Bilgi Güvenliği İhlal Olayı:** Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarıdır.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Osman VARIŞLI<br>Bilgisayar Mühendisi | Remzi BUĞDAY<br>Bilişim Uzmanı | Dr. Cihan TEKİN<br>İl Sağlık Müdürü |

- **Bilgi Güvenliği Yönetim Sistemi (BGYS) :** Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünüdür.
- **İSM**: İl Sağlık Müdürlüğü
- **SOME:** Siber Olaylara Müdahale Ekibi
- **Üst Yönetim:** Kurum adına karar verme ve harcama yetkisine sahip yönetici / yöneticilerdir.

## 5. BİLGİ GÜVENLİĞİ ORGANİZASYONU

**5.1** İSM genelinde (Müdürlüğe bağlı olan tüm sağlık teşkillerini de kapsayacak şekilde) bilgi güvenliği ve siber olaylara müdahale ile ilgili konularda en üst düzeyde karar organı olarak görev yapmak, bilgi güvenliği yetkilisi ve kurumsal SOME tarafından gerçekleştirilecek faaliyetlere destek vermek, Bakanlık tarafından yayımlanan eylem planları doğrultusunda bilgi güvenliği ile ilgili faaliyetleri takip etmek ve gerekli çalışmaları yapmak maksadıyla **İSM Bilgi Güvenliği Alt Komisyonu** oluşturulmuştur.

**5.2** Bilgi Güvenliği Alt Komisyonu çalışmalarını koordine etmek ve komisyon toplantılarına başkanlık yapmak üzere İSM'de görev yapan bir personel, Bilgi Sistemleri Koordinatörü olarak atanmıştır.

**5.3** Yönerge ve Kılavuzda belirtilen görevleri yerine getirmek ve İSM bünyesinde yer alan tüm kurum ve kuruluşlar adına Sağlık Bilgi Sistemleri Genel Müdürlüğü ile koordineli olarak gerekli çalışmaları yürütmek üzere **Bilgi Güvenliği Yetkilisi** ve **Kurumsal SOME Ekip Lideri** görevlendirilmiştir.

**5.4** İlimiz genelinde meydana gelebilecek siber olaylara müdahale etmek ve görev alanı ile ilgili hususlarda Bakanlık Sektörel SOME ile birlikte çalışmak üzere, Rehberde belirtilen esaslar çerçevesinde bir adet Kurumsal SOME oluşturulmuştur.

**5.5** Bilgi güvenliğinin insan kaynakları, fiziksel ve çevresel güvenlik, hukuk işleri ve bilgi sistemleri ile ilgili alanlarında gerekli desteği vermek üzere ilgili birimleri temsilen Bilgi Güvenliği Alt Komisyonunda komisyon üyesi olarak görev yapmak üzere personel görevlendirmesi yapılmıştır.

**5.6** Yukarıda belirtilen esaslar doğrultusunda İl Sağlık Müdürü oluru ile görevlendirilmiş personel bilgileri ektedir.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Osman VARIŞLI<br>Bilgisayar Mühendisi | Remzi BUĞDAY<br>Bilişim Uzmanı | Dr. Cihan TEKİN<br>İl Sağlık Müdürü |

**5.7** İSM'ye bağlı diğer sağlık tesislerinde bilgi güvenliği ile ilgili faaliyetler aşağıda belirtilen usul ve esaslar doğrultusunda yürütülür.

**5.7.1.** İSM'ye bağlı 2 ve 3'ncü basamak sağlık hizmeti sunumu yapan sağlık teşkillerinde bilgi güvenliği ile ilgili faaliyetleri yürütmek ve İSM Bilgi Sistemleri Koordinatörü, İSM Bilgi Güvenliği Yetkilisi ve Kurumsal SOME Lideri ile her türlü koordinasyonu yapmak üzere bir personel **Bilgi Güvenliği Yetkilisi** olarak görevlendirilir. Bilgi Güvenliği Yetkilisi görevlendirilmesi yapılırken mümkün olması halinde ilgili kurumda günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu personel dışında, Kılavuz'un A.2.4.3 maddesinde belirtilen niteliklerde bir kişinin seçilmesi tercih edilir.

**5.7.2.** 2 ve 3'üncü basamak sağlık teşkillerince, gerekiyorsa İSM Bilgi Güvenliği Alt Komisyonu ile benzer görevleri yürütmek üzere Hastane Bilgi Güvenliği Ekibi kurulur. (Kurulması halinde) Bu ekiplerde görev yapan personelin kimlik bilgileri, **Hastane Hizmet Kalite Standartları** gereği hazırlanması gereken **Hastane Bilgi Yönetim Süreç dokümanlarında** belirtilir. Bu personelin bilgilerinin, ayrıca İl Sağlık Müdürlüğüne gönderilmesine gerek bulunmamaktadır.

**5.7.3.** İSM'ye bağlı 1'inci basamak sağlık hizmeti sunumu yapan sağlık teşkillerinde ayrıca bir bilgi güvenliği yetkilisi görevlendirmesi yapılmaz. Varsa ilgili kurumda günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu olan kişi bilgi güvenliği ile ilgili faaliyetleri de yürütür. Konuyla ilgili hiçbir personeli olmayan kurum ve kuruluşların bilgi güvenliği ile ilgili faaliyetleri İSM Bilgi Güvenliği Yetkilisi tarafından yerine getirilir.

**5.8** İSM Kurumsal SOME'si, İSM'nin kendisi de dâhil İSM'ye bağlı tüm sağlık teşkillerinde meydana gelen siber güvenlik olaylarına müdahale etme ile yetkilidir. Diğer sağlık teşkillerinde bu ad altında bir ekip ya da kişi görevlendirilmesi yapılmasına gerek bulunmamaktadır.

## 6. POLİTİKA METNİ

**6.1** Diyarbakır ISM bilgi güvenliği modeli, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzuna dayanır ve kurumsal bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak için operasyonel ve yönetsel çerçeveyi sunar.

**6.2** Diyarbakır İl Sağlık Müdürü, üst yönetim adına, kurumsal faaliyetlerin icrasında iş süreçlerinin bilgi güvenliği kurallarına uygun olarak yürütülmesi için gerekli olan kaynak ihtiyaçlarını temin etmek ve bilgi güvenliğinin etkin bir şekilde uygulanmasını sağlamak hususundaki iradesini, Bilgi

Güvenliği Taahhütnamesi ile taahhüt ve beyan etmiştir. Taahhütname, https://diyarbakirism.saglik.gov.tr adresinde yer almaktadır.

**6.3** Tüm personel, faaliyetlerini dayanak kısmında belirtilen mevzuat ve başta bu politika olmak üzere üst yönetim tarafından belirlenen bilgi güvenliği politikalarına uygun şekilde yürütmekten sorumludur.

**6.4** Tüm personel, https://diyarbakirism.saglik.gov.tr adresinde yayımlanmış olan BGYS politikalarını bilmek ve gerekliliklerini uygulamakla sorumludur.

**6.5** Bilgi güvenliği ihlal olayı fark edildiğinde, https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan ihlal bildirimi internet sayfası aracılığı ile bildirilmesi tüm personelin sorumluluğundadır.

**6.6** Fiziksel güvenlik tedbirleri çerçevesinde (giriş çıkış kapıları, ofis odaları, ürün teslim alanları, depoların güvenliği ve personel tanıtım kartlarının kullanımı vb.) belirlenmiş kurallara tüm personel tarafından uyulması zorunludur.

**6.7** Bilişim altyapı hizmetlerine erişmek isteyen (sunucu erişimi, veri tabanı erişimi vb.) dış taraflar (erişime ihtiyaç duyan her türlü tedarikçi ya da Sağlık Bakanlığı dışındaki kurumlar) mutlak suretle kurum erişim prosedürüne uygun bir şekilde erişim sağlamalıdır. Uygunsuz erişim girişimleri ihlal olayı olarak tanımlanır.

**6.8** İl Sağlık Müdürlüğüne bilgi güvenliği politikası kapsamında hizmet verip bilgiye erişebilen tüm taraflar ile gizlilik sözleşmesi imzalanır.

## 7. EKLER

**7.1 Tüm Sağlık Teşkilleri Tarafından Ortak Olarak Kullanılacak Destek Dokümanları**:

- İSM Bilgi Güvenliği Organizasyonda Görev Yapan Personel Bilgileri
- Parola Politikası
- Bilgi Saklama Ortamları Yok Etme Prosedürü
- İnternet ve E-Posta Kullanım Politikası
- Sosyal Medya ve Sosyal Mühendislik Saldırılarından Korunma Politikası
- Temiz Masa, Temiz Ekran Talimatı

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Osman VARIŞLI<br>Bilgisayar Mühendisi | Remzi BUĞDAY<br>Bilişim Uzmanı | Dr. Cihan TEKİN<br>İl Sağlık Müdürü |

**7.2 Sağlık Teşkilleri Tarafından Kendi Kurumlarına Özgü Hazırlanması Gereken Destek Dokümanları**[1]:

- Erişim Kontrol Prosedürü ve Erişim Kontrol Matrisleri (yerel olarak kullanılan sistemler ve özellikle SBYS yazılımları için)
- İşe Başlama, Görev Değişikliği ve İşten Ayrılma Prosedürü (İşe Başlama Formu, İşten Ayrılma Formu vb. dâhil)
- Yedekleme Prosedürü

[1] Hastaneler tarafından kullanılacak dokümanlar, Hastane kalite süreçleri kapsamında hazırlanan "hastane bilgi yönetim sistemi politikaları" içerisinde veya ayrı destek dokümanları şeklinde hazırlanabilir.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Osman VARIŞLI<br>Bilgisayar Mühendisi | Remzi BUĞDAY<br>Bilişim Uzmanı | Dr. Cihan TEKİN<br>İl Sağlık Müdürü |