

**SAĞLIK BAKANLIĞI**  
**SAĞLIK BİLİMLERİ ÜNİVERSİTESİ**  
**BAĞCILAR EĞİTİM VE ARAŞTIRMA HASTANESİ**  
**BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ**  
**BİRİNCİ BÖLÜM**

**Amaç, Kapsam, Dayanak ve Tanımlar**

**Amaç**

**MADDE 1-** (1) Bu Yönergenin amacı, bilginin işlenmesi süreçlerinde bilgi güvenliğinin sağlanmasına yönelik tedbir almak; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak; yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesinde bilgi güvenliği açısından uyulması gereken usul ve esasları belirlemektir.

**Kapsam**

**MADDE 2-** (1) Bu Yönerge, hastanemizde görev yapan tüm personel ile kendilerine herhangi bir nedenle hastanemiz bilgi ve bilgi işleme tesislerine erişim yetkisi verilenleri, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini, hizmet sağlayıcılarını, sistem, veri ve bilgi kullanıcılarını ve kurallarını kapsar.

**Dayanak**

**MADDE 3-** (1) Bu Yönerge, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 ıncı maddesinin birinci fıkrasına dayanılarak hazırlanmıştır.

**Tanımlar**

**MADDE 4-** (1) Bu Yönergenin uygulanmasında;

- a) Bilgi: Kurum için değeri olan, uygun bir şekilde korunması gereken, yazılı olarak veya bilgi sistemleri üzerinde işlenen tüm kaynakları,
- b) Bilgi işleme: Veri ve bilgilerin manuel veya bir otomasyon sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri ve bilgiler üzerinde gerçekleştirilen her türlü işlemi,
- c) Bilgi işleme tesisi: Bilgi işlemede kullanılan her türlü sistem, servis, altyapı ve

bunların konuşlandırıldığı fiziksel mekânları,

- d) 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 tümünü,
- e) Bilgi güvenliği yetkilisi: İlgili kurumdaki alt komisyon tarafından görevlendirilen ve komisyon adına bilgi güvenliği politikalarının uygulanması için yetki verilen kişiyi,
- f) Bilgi güvenliği yönetim sistemi: 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 bütünü,
- g) Bilgi sistemleri: Donanım, yazılım, veri, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütünü,
- h) BGYS: Bilgi güvenliği yönetim sistemini,
- i) Kılavuz: Bilgi Güvenliği Politikaları Kılavuzunu,
- j) Kullanıcı: Hastanemizde yer alan bilgi ve bilgi işleme tesislerine erişen tüm kişileri,
- k) Kurumsal SOME: Sektörel SOME tarafından belirlenen ve kritik altyapı işleten kurumlarda kurulan siber olaylara müdahale ekibini,
- l) Rehber: Kurumsal SOME Kurulum ve Yönetim Rehberini,
- m) Sızma testi: Bilişim sistemleri üzerinde, saldırgan bakış açısıyla güvenlik zafiyetlerinin tespit edilip bulunan zafiyetlerin kullanılarak sistemlere sızılmaya çalışılması ve raporlanması işlemlerini,
- n) Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,
- o) Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,
- p) Siber olay: Bilgi sistemleri ve endüstriyel kontrol sistemleri (ağa bağlanabilen

diğer cihazlar, tıbbi cihazlar vb.) veya bu sistemlerde tutulan veya işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

- q) Siber olaya müdahale: Bilgi sistemleri ve endüstriyel kontrol sistemleri (ağa bağlanabilen diğer cihazlar, tıbbi cihazlar vb.) veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinde meydana gelme riski bulunan veya meydana getirilen siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları,
- r) SOME: Siber olaylara müdahale ekibini,
- s) SOME ekip lideri: İlgili kurumun bilgi güvenliği yönetim komisyonu tarafından görevlendirilen, kurumsal SOME faaliyetlerini yürütmekle görevli kişiyi,
- t) Sektörel SOME: Bakanlık bünyesinde kurulan siber olaylara müdahale ekibini,
- u) Sosyal mühendislik testi: Kurum çalışanlarının kişisel hesaplarının güvenliği ve bilgi güvenliği politikaları ile ilgili farkındalık seviyelerini ölçmek için yapılan, senaryoları önceden paylaşılmış kontrolleri,
- v) Veri: Bilginin işlenmemiş halini,

ifade eder.

## İKİNCİ BÖLÜM

### Temel İlkeler

#### Temel ilkeler

**MADDE 5-** (1) Hastanemizde yer alan birimlerde, başta kişisel sağlık verileri olmak üzere, yazılı veya elektronik ortamda saklanan her türlü bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla BGYS tesis edilir.

(2) BGYS'nin tesis edilmesi ve etkin bir şekilde işletilmesi için, üst yönetim desteği ve katılımı zorunludur. Hastanemiz idaresi bu Yönergenin dördüncü bölümünde belirtilen bilgi güvenliği organizasyonunun kurulmasından ve kendilerine bağlı en uç noktalara kadar bilgi güvenliği ile ilgili tedbirlerin alınmasını sağlamaktan birinci derecede sorumludur.

(3) BGYS tesis edilmesi için alınması gereken tedbirler, Kılavuzda yer alan bilgi güvenliği politikaları ve kurumların kendilerine özgü güvenlik ihtiyaçları dikkate alınmak suretiyle ayrıntılı olarak belirlenir, yazılı hale getirilir ve tüm kullanıcılara duyurulur.

- (4) Tesis edilen BGYS için herhangi bir belgelendirme kuruluşundan sertifika alınması zorunlu değildir.
- (5) Etkin bir BGYS tesis edilmesi için risk yönetimi yapılır. Tespit edilen riskler için riski azaltacak veya kaldıracak tedbirler belirlenir ve uygulanır. Risk yönetimi süreçleri süreklilik arz eder.
- (6) Bilgi işleme faaliyetlerinin büyük oranda siber ortam üzerinden yapılması nedeniyle, siber güvenlik tedbirlerinin alınması için azami özen gösterilir.
- (7) Bilgi güvenliğinin sağlanması için sadece siber güvenlik ile ilgili tedbirlerin alınması yeterli değildir. Personel, evrak, ekipman, fiziksel ve çevre güvenliği için de güvenlik tedbirleri alınması gerekir.
- (8) Kullanıcılar, görev yaptıkları kurumun BGYS politikalarına uymak ve görevlerini ifa ederken öğrenmiş oldukları bilgileri, sır saklama yükümlülüğü uyarınca süresiz olarak saklamakla yükümlüdür.
- (9) BGYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında 657 sayılı Devlet Memurları Kanunu'nun veya iş sözleşmesinin ilgili hükümleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ilgili hükümleri uyarınca işlem yapılır.

## ÜÇÜNCÜ BÖLÜM

### Kılavuz, Rehber ve Uygulanması

#### Kılavuz ve Rehberin hazırlanması ile değişikliklerin yönetimi

**MADDE 6-** (1) Hastanemiz tarafından, Yönerge'de yer alan konuları açıklamak ve uygulamaya yönelik esasları belirlemek üzere, Bilgi Güvenliği Politikaları Kılavuzu ve Kurumsal SOME Kurulum ve Yönetim Rehberi hazırlanır.

- (2) Kılavuz ve Rehber, Hastanemiz internet sitesinde yayımlanır.
- (3) Kılavuz ve Rehber, planlanan zaman aralıklarında veya teknik gereklilikler ortaya çıktığında uygunluğu, elverişliliği ve etkinliğinin sürekliliğini belirlemek amacıyla Genel Müdürlükçe oluşturulacak çalışma grupları vasıtasıyla gözden geçirilir.
- (4) Kılavuz ve Rehberin yeniden bir bütün olarak yayımlanmasını gerektirmeyen küçük çaplı değişiklikler, değişiklik eki olarak hazırlanır. Değişiklik ekleri, dokümanların yürürlükteki sürümleri üzerine işlenmek suretiyle takip edilir.
- (5) Dokümanlarda önemli ölçüde değişiklik yapılmasını gereken durumlarda, yeni sürümler bir bütün olarak yayımlanır.

#### Kılavuz ve Rehberin uygulanması

**MADDE 7-** (1) Kılavuz ve Rehberde yer alan hususların hayata geçirilmesi ve takibi

için Hastanemiz tarafından eylem planları hazırlanır ve yayımlanır.

(2) Hastanemizce, eylem planında belirtilen konularda çalışmalar yapılır ve neticeleri, planda belirtilecek süreçlere uygun olarak İl Sağlık Müdürlüğüne bildirilir.

## **DÖRDÜNCÜ BÖLÜM**

### **Bilgi Güvenliği Organizasyonu**

#### **Bilgi Güvenliği Yönetim Komisyonu**

**MADDE 8-** (1) Hastanemiz genelinde, bilgi güvenliği ve siber olay yönetimi ile ilgili konularda en üst düzeyde koordinasyon ve karar organı olarak görev yapmak üzere Bilgi Güvenliği Yönetim Komisyonu kurulur.

(2) Komisyon; Hastanemiz yöneticileri, birim sorumluları ve bilgi işlem birimi personellerinden oluşur.

(3) Komisyon, ulusal siber güvenlik stratejisi ve eylem planı uyarınca, kritik sektörler arasında yer alan sağlık sektörü ile ilgili siber güvenlik stratejilerinin belirlenmesi ve Bakanlık dışındaki diğer paydaşlar ile koordine edilmesi faaliyetlerini de yürütür.

(4) Komisyonun üyeleri, görev, sorumluluk ve çalışma usulleri Kılavuz ile düzenlenir.

#### **Alt komisyonlar**

**MADDE 9-** (1) Hastanemiz bünyesinde, bilgi güvenliği ve siber olaylara müdahale faaliyetlerini yürütmek ve koordine etmek üzere, Hastanemiz bünyesinde oluşturulan Komisyona benzer şekilde bilgi güvenliği alt komisyonları oluşturulur.

(2) Alt komisyonların çalışmalarında bilgi güvenliği yetkilisi ve kurumsal SOME ekip liderine ilave olarak; kurumların bilgi işlem ve istatistik, insan kaynakları, kalite, hukuk ve fiziksel güvenlikten sorumlu birimlerinin yöneticileri de komisyon üyesi olarak yer alır. Ayrıca gerekli görülecek diğer personel de alt komisyonlarda yer alabilir.

#### **Bilgi güvenliği yetkilisi**

**MADDE 10-** (1) Hastanemiz bünyesinde, alt komisyonlar adına bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere "bilgi güvenliği yetkilisi" görevlendirilir.

(2) Hangi seviyede ve hangi alt kuruluşlarda "bilgi güvenliği yetkilisi" görevlendirileceği, ilgili alt komisyonlar tarafından karar altına alınır. Bu tespit yapılırken kurum bilgi işleme tesisleri, personel sayısı, bölgesel özellikler, tespit edilen risklerin miktarı ve önem derecesi gibi ölçütler göz önüne alınarak, ölçek yaklaşımı

çerçevesinde karar verilir ve görevlendirilen bilgi güvenliği yetkilisinin sorumluluk kapsamı belirlenir.

## **BEŞİNCİ BÖLÜM**

### **Bilgi Güvenliği İhlal Olaylarının Yönetimi ve Denetim**

#### **Bilgi güvenliği ihlal olaylarının yönetimi**

**MADDE 12-** (1) Hastanemiz çalışanları ve vatandaşlar tarafından tespit edilen Hastanemiz ile ilgili her türlü bilgi güvenliği ihlal olayı, Hastanemiz bilgi işlem birimine iletilir.

(2) Bildirilen olaylar, Hastanemiz ekipleri tarafından değerlendirilir. Hastanemizi ilgilendirecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına zarar verebilecek ihlal olaylarına Hastanemiz işlem yapılır ve neticesi bildirim yapan kişiye iletilir.

#### **Bilgi güvenliği denetimi**

**MADDE 13-** (1) Hastanemiz, kapsam maddesinde belirtilen tüm unsurlarla ilgili olarak, Kılavuzda belirtilen konularda, planlı bilgi güvenliği denetimleri yapar veya yaptırır.

(2) Hastanemiz, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, sektörel SOME vasıtasıyla Hastanemizde sızma ve sosyal mühendislik testleri gerçekleştirir.

(3) Hastanemiz, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, kurumsal SOME vasıtasıyla kendi bağlı birimlerde sızma ve sosyal mühendislik testleri yapar veya yaptırır.

(4) Hastanemiz, bilgi güvenliği denetimi ile sızma ve sosyal mühendislik testi yapacak personelin niteliklerini belirler.

## **ALTINCI BÖLÜM**

### **Bilgi Güvenliği ve SOME Eğitimleri**

#### **Eğitimler**

**MADDE 14-** (1) Hastanemiz tarafından bilgi güvenliği / siber güvenlik konularına yönelik eğitim, tatbikat, seminer, konferans, sempozyum gibi faaliyetler planlanır ve uygulanır. Ulusal ve uluslararası düzeyde planlanan benzeri etkinliklere İl Sağlık Müdürlüğü koordinatörlüğünde katılım sağlanabilir.

(2) Hastanemizde görev yapan personelin bilgi güvenliği farkındalık seviyesinin artırılması amacıyla ihtiyaç duyulan eğitimler, Eğitim Birimi tarafından planlanır ve

uygulanır.

(3) Kurumsal SOME'lerin alması gereken eğitimler, sektörel SOME tarafından organize edilir.

## YEDİNCİ BÖLÜM

### Çeşitli ve Son Hükümler

#### Bilgi güvenliği ve standartları

**MADDE 15-** (1) Hastanemiz, bilgi güvenliği çalışmalarının standardize edilmesi ve çalışmalara sistematik bir anlayış getirilmesi için çalışır. Bu amaç ile konuya ilişkin ulusal ve uluslararası standartları kullanır, bunu belgeleyen sertifikaların temini yönünde çalışmalar yapar. Bu konuda ulusal ve uluslararası kuruluşlarla iş birliği gerçekleştirir.