T.C.
SAĞLIK BAKANLIĞI

BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönergenin amacı; Sağlık Bakanlığı'nın, görevleri kapsamında; bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesinde bilgi güvenliği açısından uyulması gereken usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönerge, Bakanlık ve bağlı kuruluşları, merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve misafir kullanıcıları, bilgi sistemleri unsurlarını, insan kaynaklarını, bilgi sistemleri ile ilgili mal ve hizmet alımlarındaki güvenlik unsurlarını, hizmet sağlayıcıları, sistem, veri ve bilgi kullanıcılarını ve kurallarını kapsamaktadır.

Dayanak

MADDE 3- (1) Bu Yönerge, 663 sayılı "Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin" 11 inci maddesinin birinci fıkrasının (ç) bendine ve "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında 5651 sayılı Kanun'un" 6'ncı maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE4- (1) Bu Yönergenin uygulanmasında;

a) Bakan : Sağlık Bakanını,
b) Bakanlık : Sağlık Bakanlığını,
c) Bağlı Kuruluş : Türkiye Halk Sağlığı Kurumu, Türkiye İlaç ve Tıbbî Cihaz Kurumu, Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü ve Türkiye Kamu Hastaneleri Kurumu'nu,
ç) Genel Müdürlük : Sağlık Bilgi Sistemleri Genel Müdürlüğü'nü,
d) KHK : 663 Sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnameyi,
e) Kılavuz : Bilgi Güvenliği Politikaları Kılavuzunu,
f) Komisyon : Bilgi Güvenliği Yönetim Komisyonu'nu
g) Kullanıcı : Bakanlık ve bağlı kuruluşları Bilgi Sistemlerini kullanan tüm kişileri,
ğ) Bilgi : Kurum için değeri olan, uygun bir şekilde korunması gereken tüm kaynakları,
h) Veri : Bilginin işlenmemiş halini,
ı) Bilgi güvenliği : Bilgi ve bilginin işlem gördüğü bilgi sistemlerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz

şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümünü,

i) Bilgi Güvenliği Yetkilisi : İlgili kurumun üst düzey yöneticisi tarafından Bilgi Güvenliği Politikalarının uygulanması için yetki verilen kişiyi,

j) Bilgi Sistemleri : Donanım, yazılım, veri, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü,

k) Hizmet Sağlayıcıları : Kurum adına bir işi yapmayı üstüne alan firmayı ya da kişiyi,

m) Sosyal Mühendislik Testi: Kurum çalışanlarının kişisel hesaplarının güvenliği ve bilgi güvenliği politikaları ile ilgili farkındalık seviyelerini ölçmek için yapılan, senaryoları önceden paylaşılmış kontrolleri,

ifade eder.

İKİNCİ BÖLÜM
Temel İlkeler

MADDE 5- (1) Tüm yöneticiler, yönetim alanları ve yerine getirmekle yükümlü oldukları tüm iş ve işlemlerin yürütülmesinde kullandıkları bilgi sistemleri ile ilgili olarak; bilgi güvenliği duyarlılığı çerçevesinde hareket etmekle, yönetim alanları ve işleri ile ilgili olarak bilgi güvenliği iş planı hazırlamakla ve yürürlüğe koymakla yükümlüdürler.

(2) Her kullanıcı, Kılavuzda yer alan kişisel veya çalışma alanı ile ilgili hususlara uymakla yükümlüdür.

(3) Kullanıcı, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabileceği konularında bilinçli olmalıdır.

(4) Tüm yöneticiler, kendi sorumluluk alanlarındaki bilgi sistemleri ve ağlarının güvenliğinden sorumludurlar.

(5) Kullanıcı, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmekten sorumludur.

(6) Kullanıcılar, bilgi sistem ve ekipmanlarının kullanımında birbirlerinin haklarına saygı göstermekle yükümlüdürler.

(7) Kullanıcı, idarece yapılmış olan risk değerlendirmelerinde kendileriyle ya da çalışma alanlarıyla ilgili öngörülen tedbirlere uymak zorundadır.

(8) Güvenlik, bilgi sistem ve ağlarının önemli bir unsuru olarak değerlendirilmelidir.

(9) Bilgi sistem ve ağlarının güvenliği sürekli olarak izlenir ve değerlendirilir. Bu değerlendirme neticesinde, güvenliğin gerekli kıldığı değişiklikler zamanında yapılır.

ÜÇÜNCÜ BÖLÜM
Bilgi Güvenliği Politikası

MADDE 6- (1) Bilgi güvenliği politikası, bilgi güvenliği kapsamındaki yetki ve sorumlulukların dağıtılmasında hukuki araç olarak kullanılacak bir doküman olarak Bakanlık ve bağlı kuruluşlar adına Genel Müdürlükçe hazırlanmak suretiyle Kılavuzun içinde yer alır.

(2) Bu Yönergeye bağlı olarak hazırlanacak olan Kılavuz Bakanlık internet sitesinde bulundurularak Bakanlık ve bağlı kuruluşlar ve bunların taşra teşkilatındaki tüm personelin Kılavuzdan bilgi sahibi olması sağlanır.

(3) Bu Yönergeye bağlı olarak Genel Müdürlükçe hazırlanacak ve yayımlanacak olan Kılavuz, planlanan zaman aralıklarında veya teknik gereklilikler ortaya çıktığında, uygunluğu, elverişliliği ve etkinliğinin sürekliliğini belirlemek için gözden geçirilir.

(4) Gözden geçirme neticesinde; Kılavuz ile ilgili olarak revizyon yapılması gerektiğinde, Genel Müdürlükçe oluşturulacak komisyon tarafından revize edilerek yayımlanır.

DÖRDÜNCÜ BÖLÜM
Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği Yönetim Komisyonu

MADDE 7- (1) Genel Müdürlük tarafından, bilgi güvenliğinin iç organizasyonunun sağlanması için bilgi güvenliği konusunda uzmanlaşmış, bilgi sistemlerinin kapsamı göz önüne alınarak, teknik, idari ve hukuki süreçlerde çalışmalarda bulunmak üzere "Bilgi Güvenliği Yönetim Komisyonu" oluşturulur.

(2) Komisyona bağlı olarak çalışmak üzere bilgi güvenliğinin farklı alt alanlarında "çalışma grupları" teşkil edilir. Çalışma grupları oluşturulurken teknik, hukuki ve idari disiplinlerden personel bulunmalıdır.

(3) Komisyonun görevleri şunlardır;

a) Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde bu Yönergeye bağlı olarak çalışma grupları tarafından hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını verir,

b) Bilgi güvenliği politikalarının uygulanmasının etkinliğini ölçer,

c) Bilgi güvenliği faaliyetlerinin yürütülmesinde rehberlik yapar,

ç) Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,

d) Yönerge kapsamındaki bilgi güvenliği faaliyetlerini koordine eder.

Bilgi Güvenliği Yetkilisi

MADDE 8-(1) Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları kurumları bünyesinde, bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere "Bilgi Güvenliği Yetkilisi " görevlendirilir. Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları üst yönetimleri hangi seviyede ve hangi alt kuruluşlarında "Bilgi Güvenliği Yetkilisi" görevlendireceklerine kurum bilgi sistemleri kapsamı, etki alanı, personel sayısı gibi kriterleri göz önüne alarak, ölçek yaklaşımı çerçevesinde karar verirler ve görevlendirecekleri Bilgi Güvenliği Yetkilisinin sorumluluk kapsamını belirlerler.

(2) Bilgi Güvenliği Yetkilisinin ana işlevi; bulunduğu kurumdaki bilgi güvenliği faaliyetlerini Genel Müdürlük ile koordineli bir şekilde yürütmektir. Bilgi Güvenliği Yetkilisi olarak görevlendirilen personel Genel Müdürlük tarafından ana ilke ve politikalar konusunda eğitilir ve yönlendirilir.

(3) Bilgi güvenliği ihlal bildirimleri anında Bilgi Güvenliği Yetkilisine bildirilir. Bilgi Güvenliği Yetkilisi, Kurumu için Kılavuz çerçevesinde "Bilgi Güvenliği Planı" yapar ve bu Plan görev yaptığı kurum idaresince onaylanır.

BEŞİNCİ BÖLÜM
Bilgi Güvenliği İhlali Yönetimi ve Denetim

Bilgi Güvenliği İhlali Yönetimi

MADDE 9- (1) Bilgi güvenliği olaylarının rapor edilmesi;

a) Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan idari uygulama planı oluşturulur.

b) Bilgi güvenliği ihlalini bildirmek üzere bir rapor formatı hazırlanır.

c) Güvenlik ihlal olayının oluşması durumunda, olay anında raporlanır.

ç) Güvenlik ihlaline neden olanlar hakkında, hukuki süreç başlatılır.

(2)Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını

önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor ederler.

Bilgi Güvenliği Denetimi

MADDE 10- (1) Genel Müdürlük kapsam maddesinde belirtilen tüm unsurlarla ilgili Kılavuzda belirtilen hususlarda bilgi güvenliği denetimleri yapar.

(2) Bilgi güvenliği denetimlerini yapacak personelin nitelikleri Genel Müdürlükçe belirlenir.

(3) Senaryoları idarece önceden onaylanmak kaydıyla "bilişim güvenliği ve sosyal mühendislik testleri" yapılabilir.

(4) Genel Müdürlük, bilgi güvenliği denetimlerinde yer almak üzere yeteri kadar personelin eğitimi ile ilgili çalışmaları yapar.

ALTINCI BÖLÜM
Bilgi Güvenliği Politikaları Kılavuzu ve Uygulanması

Bilgi Güvenliği Politikaları Kılavuzu

MADDE 11- (1) Kılavuz; Genel Müdürlük tarafından kapsam maddesinde tanımlanan tüm unsurlarla ilgili olarak; bilgi güvenliğinin sağlanması ile ilgili; yönetsel, teknik, idari, hukuki süreçlerin tüm detaylarının yer alacağı bir doküman olarak hazırlanır.

(2) Kılavuzun ilk versiyonu Bakanın onayı ile yürürlüğe girer.

(3) Kılavuz; periyodik olarak, teknolojik gelişmeler paralelinde gözden geçirilerek revize edilir ve elektronik ortamda yayımlanacak bir rehber doküman olarak hazırlanır.

(4) Kapsam maddesinde belirtilen tüm Bakanlık ve bağlı kuruluşları Kılavuzda yer alan hususlara uymakla yükümlüdürler. Gerekli hallerde Genel Müdürlükçe teknik destek talepleri karşılanır. Genel Müdürlük, Bakanlık internet ana sayfası üzerinde bilgi güvenliği bağlantı adresi oluşturur. Bu bağlantı adresi üzerinden açılan internet sayfasında bilgi güvenliği konularında üretilen ulusal ve uluslararası kılavuz, rapor, bilgi notu, tez vb. dokümanlarına erişim sağlanır.

(5) Genel Müdürlük, Bilgi Güvenliği Terimleri Sözlüğü hazırlar ve internet üzerinden yayıma sunar.

Kılavuzun Uygulanması

MADDE 12- (1) Kılavuzun uygulanması ile ilgili olarak; yöneticiler hazırlayacakları bilgi güvenliği planları içerisinde "Kılavuza Uyumlaşma Takvimi " hazırlar ve kılavuzun uygulanması ile ilgili gerekli idari tedbirleri alır.

YEDİNCİ BÖLÜM
Bilgi Güvenliği Eğitimleri

MADDE 13- (1) Genel Müdürlük, bilgi güvenliği eğitim planlamasını tüm Bakanlık ve bağlı kuruluşları için yapmak suretiyle her seviyedeki personelin bilgi güvenliği farkındalık düzeylerini artırmak yönünde eğitim faaliyetlerinde bulunur. Yıllık hizmet içi eğitim planlamalarında bilgi güvenliği başlığı planlara dahil edilir. Teknik seviyedeki personelin bilgi düzeyinin artırılması yönünde ileri seviyede bilgi güvenliği eğitim planlamalarını yapar.

(2) Ulusal düzeyde siber güvenlik ile ilgili kurum ve kuruluşlarla ortak eğitim, seminer, konferans, sempozyum gibi faaliyetler gerçekleştirilmesine yönelik yıllık planlar yapar.

(3) Bilgi güvenliği ile ilgili uzaktan eğitim modülünü devreye sokarak, teknik ve farkındalık eğitimlerini web tabanlı olarak sunar.

SEKİZİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Bilgi Güvenliği Standartları

MADDE 14- (1) Genel Müdürlük bilgi güvenliği çalışmalarının standartlaştırılması ve çalışmalara sistematik bir anlayış entegre edilmesi yaklaşımı ile ulusal ve uluslararası bilgi güvenliği standartlarına uyumlaşmanın ve sertifikasyonun gerçekleştirilmesi yönünde çalışmalar yapar. Bu konuda ulusal ve uluslararası kuruluşlarla işbirliği gerçekleştirir.

Yürürlük

MADDE 15- (1) Bu Yönerge, Sağlık Bakanının onayı ile yürürlüğe girer.

Yürütme

MADDE 16- (1) Bu Yönerge hükümlerini Sağlık Bakanı yürütür.