1. **AMAÇ**

BGYS politikası, T.C. Sağlık Bakanlığı, İl Sağlık Müdürlüğü ve bağlı tesisleri bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir.

2. **KAPSAM**

Bu politika Kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamakla birlikte;

Veri dosyaları, sözleşmeler vb. den oluşan bilgi varlıkları,

Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,

Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,

Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,

Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıklarını kapsamaktadır.

3. **BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ**

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

3.1.HEDEF

1. Kurumu içeriden veya dışarıdan gelebilecek tehditlere karşı korumak, üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak kurumun imajını korumak,
2. Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak,
3. Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
4. Bilgi Güvenliği prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırmak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

3.2.BİLGİ GÜVENLİĞİ İLKELERİ

1. Bilgi güvenliği ilkeleri, kurumdaki bilgi güvenliği ile ilgili genel kuralları koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.

2. Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:
3. Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
4. Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
5. Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
6. Bilgi güvenliği ihlal olaylarını Bilgi Güvenliği Yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
7. 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.
8. Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
9. Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacı kullanılamaz.
10. Kurumun tüm çalışanları; bu politikaya, prosedür ve talimatlarına uymakla sorumludur.
11. İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
12. Bilgilerin bütünlüğü her durumda korunacaktır.
13. Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
14. Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
15. Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.

4. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Sağlık Bakanlığı **İl Sağlık Müdürlüğü** bünyesinde bu politika metninde tarif edilen kapsam dahilinde Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS KOMİSYONU ve BGYS ÇALIŞMA GRUBU kurulmuştur.

4.1.BGYS ALT KOMİSYONU VE ÇALIŞMA GRUBU

ADI SOYADI	ÜNVANI	GÖREVİ
	Destek Hizmetleri Başkan Yardımcısı	Bilgi Sistemleri Koordinatörü
Serkan ASLANALP	Mühendis	Bilgi Güvenliği Yetkilisi
Sırrı Özgür AYDOĞ	Uzman	Bilgi Güvenliği Yetkilisi (Yedek)
Sırrı Özgür AYDOĞ	Uzman	Kurumsal Some Ekip Lideri
Şenol Sarıca	Teknik Personel	Kurumsal Some Ekip Lideri (Yedek)

4.2. KURUM ORGANİZASYON ŞEMASI

4.3 BG ÜST YÖNETİM GÖREV, YETKİ VE SORUMLULUKLARI

1. Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.
2. Bilgi güvenliği birimi tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için BGYS (Bilgi Güvenliği Yönetim Sistemi) Birimi tarafından hazırlanmış projelere gerekli kaynağı sağlamak.
3. BGYS Birimi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.
4. BGYS Birimi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.
5. Çalışmaların yürütülebilmesi için yatırım kararlarına, **İl Sağlık Müdürlüğü** Birimlerinde ve üçüncü taraf hizmet alımlarında BGYS birimi tarafından çalışılan uluslararası standartlar çerçevesinde yapılması gereken çalışma süreçleri, usul ve esaslara dair değişiklikleri onaylamak.
6. Belirli aralıklarla yapılacak olan BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.
7. Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (Danışmanlar ve yüklenici firma personeli dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.
8. Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.
9. BGYS Birimi tarafından hazırlanmış, BGYS Komisyonu tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

4.4.BGYS KOMİSYON BAŞKANI GÖREV, YETKİ VE SORUMLULUKLARI

1. Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.
2. Çalışmaların yürütülebilmesi için gerekli komisyonu oluşturmak ve görev tanımlarını yapmak.
3. Bilgi Güvenliği Komisyonuna başkanlık etmek.
4. Bilgi Güvenliği Komisyonundan gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
5. Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.

4.5.BGYS KOMİSYONU GÖREV, YETKİ VE SORUMLULUKLAR

1. BGYS Komisyonu BGYS Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.

2. BGYS Yönetim Temsilcisi bu komisyona başkanlık eder.
3. Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek.
4. T.C. Sağlık Bakanlığına bağlı diğer birimlerde ve tüm taşra teşkilatında uygulanması gereken Bilgi güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak. BGYS yönetim temsilcisi ve BGYS birimi tarafından gerekli görüldüğünde toplantılara katılmak.
5. Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.
6. BGYS birimi tarafından hazırlanan projelerin gerekliliği olan, birim çalışanlarının, danışmanların ve yüklenici firma personellerinin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

4.6.BGYS BİRİMİ GÖREV, YETKİ VE SORUMLULUKLARI

1. Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.
2. **İl Sağlık Müdürlüğü'ne** bağlı diğer birimlerde ve tüm taşra teşkilatında uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve katkı sunmak.
3. **İl Sağlık Müdürlüğü'ne** bağlı diğer birimlerde ve tüm taşra teşkilatı ile ilgili yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
4. Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerine katılmak, dokümantasyon geliştirme faaliyetlerinde yer almak.
5. Projelerin yürütülebilmesi için gerektiğinde, komisyon toplantısı, çalışma grupları toplantısı, yüklenici firma ziyareti birim ziyareti, taşra teşkilatı ziyareti gibi ziyaretlerin organize edilmesi gerekli yasal izinlerin alınması gerekli araç izinlerinin alınması gibi hususlarda gerekli organizasyonları yapar.
6. **İl Sağlık Müdürlüğü'ne** bağlı birimlerde ve taşra teşkilatında yapılacak olan çalışmaların proje planlarının hazırlanması, gerekli bilgilendirme raporları, sunumları ve eğitimlerin organize edilmesi ve gerçekleştirilmesi konularında rehberlik etmek ve katkı sunmak.
7. Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerini yerine getirme hususunda çalışmalara katılmak hazırlanan dokümantasyonun ilgili taraflar tarafından okunmasını ve anlaşılmasını sağlamak.
8. Projeler kapsamında yapılacak olan farkındalık eğitimi, temel eğitim, iç denetçi eğitimi gibi konular gereği gerekli düzenlemeleri ve organizasyonları yapmak, eğitim değerlendirmeleri yapmak, katılımcı imzalarının alınmasını sağlamak.