1. AMAÇ

Bu politika İstanbul il Sağlık Müdürlüğü ve bağlı tüm 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; İstanbul il Sağlık Müdürlüğü ve bağlı tüm sağlık tesislerinde 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 Resmî 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.
- 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: İstanbul İl Sağlık Müdürlüğü
- SOME: Siber Olaylara Müdahale Ekibi
- Üst Yönetim: Kurum adına karar verme ve harcama yetkisine sahip yönetici / yöneticilerdir.
- YGG: Yönetimi Gözden Geçirme

5. BİLGİ GÜVENLİĞİ ORGANİZASYONU

İstanbul il Sağlık Müdürlüğü ve bağlı tüm tesislerinde 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 yapabilmek için İSM Bilgi Güvenliği Alt Komisyonu oluşturulmuştur.

Bilgi Güvenliği Alt Komisyonu çalışmalarını koordine etmek ve komisyon toplantılarına başkanlık yapmak üzere İSM Destek Hizmetleri Başkan Yardımcısı Bilgi Sistemleri Koordinatörü olarak görevlendirilmiştir.

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.

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 Kurumsal SOME oluşturulmuştur.

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 görev yapmak üzere aşağıda belirtilen personeller görevlendirilmiştir.

İSM Bilgi Güvenliği Alt Komisyonu

Komisyon Başkanı: Serdal ZELYURT (Bilgi Sistemleri Koordinatörü)

Üye: Şeri AYRANCIOĞLU (Bilgi Sistemleri Birim Sorumlusu)

Üye: Çağrı AKAR (Bilgi Güvenliği Yetkilisi)

Üye: Yakup YİĞİDER (Kurumsal SOME Ekip Lideri) Üye:

Halil Çağrı DiNÇ

Üye: Murat KONUK

Üye: Başak ÇOBANOĞLU

Üye: Tevfik KESEMEN

Üye: Musa AYKAÇ

Üye: Ufuk BEKAR Üye:

Sebahattin UZUN

Üye: Umut DEMIROĞLU

Üye: Özkan TÜM (Avukat)

Yukarıda belirtilen esaslar doğrultusunda oluşturulan organizasyon şeması aşağıda yer almaktadır.

İstanbul İl Sağlık Müdürlüğü Bilgi Güvenliği Organizasyon Şeması

İstanbul İl Sağlık Müdürlüğü 'ne bağlı diğer tüm sağlık tesislerinde bilgi güvenliği ile ilgili faaliyetler aşağıda beliÛilen usul ve esaslar doğrultusunda yürütülür.

İSM BGYS Politikası ve Polıtikanın 11.1. maddesinde **belirtilen bağlı** sağlık tesisleri tarafından ortak kullanılacak destek dokümanları İstanbul İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesisleri için geçerlidir. Bağlı sağlık tesisleri BGYS Politikası ve politikanın 11.1. maddesinde belirtilen dokümanları kurumuna özgü oluşturamaz.

İstanbul İl Sağlık Müdürlüğü 'ne bağlı 2 ve 3'üncü basamak sağlık tesislerinde, bilgi güvenliği ile ilgili faaliyetleri yürütmek, İSM Bilgi Sistemleri Koordinatörü, İSM Bilgi Güvenliği Yetkilisi ve İSM Kurumsal SOME Ekip Lideri ile her türlü koordinasyonu yapmak üzere bir personel Bilgi Güvenliği Sorumlusu olarak görevlendirilir. İlgili sağlık tesisinde görevlendirilen bu personellerin yazıları İstanbul il Sağlık Müdürlüğü 'nde bulunmaktadır.

İstanbul İl Sağlık Müdürlüğü 'ne bağlı 2 ve 3'üncü basamak sağlık tesislerinde, İSM tarafından ayrıca bir Bilgi Güvenliği Ekibi oluşturulmamıştır. Ayrıca, Sağlık Kalite Standartlarında da belirtilen bilgi güvenliği konularındaki faaliyetleri yürütebilmek adına sağlık tesisinde Bilgi Güvenliği Ekibi kurulması ilgili İdare 'nin sorumluluğundadır. Kurulması halinde personel bilgilerinin Hastane Bilgi Yönetim Süreç Dokümanları 'nda belirtilmesi yeterli olup ayrıca il Sağlık Müdürlüğü 'ne gönderilmesi gerekmemektedir. Kurulması halinde ilgili sağlık tesisindeki bilgi güvenliği ekibi, tesis ile ilgili risk değerlendirmesi, altyapı güvenliği, SBYS güvenliği, kişisel verilerin korunması vb. konularda karar alabilir. Fakat, alınacak kararlar İSM BGYS Politikası ve 11.1. maddesinde **belirtilen** ortak kullanılacak destek dokümanlarına aykırı olamaz.

İstanbul İl Sağlık Müdürlüğü 'ne bağlı 1'inci basamak sağlık tesislerinde ayrıca bir bilgi güvenliği sorumlusu görevlendirmesi yapılmayacaktır. İlgili sağlık tesisinde günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu olan kişi aynı zamanda bilgi güvenliği ile ılgilı faaliyetleri de yürütecektir. Konuyla ilgili sorumlu personeli olmayan tesislerin bilgi güvenliği ile ilgili faaliyetleri İSM Bilgi Güvenliği Yetkilisi tarafından yerine getirilir.

İSM Kurumsal SOME 'si, İstanbul il Sağlık Müdürlüğü ve bağlı tüm sağlık tesislerinde meydana gelen tüm siber güvenlik olaylarına müdahale etme ile yetkilidir. Diğer sağlık teşkillerinde bu ad altında bir ekip ya da kişi görevlendirilmesi yapılmasına gerek bulunmamaktadır.

6. ÜST YÖNETİM GÖREV, YETKİ VE SORUMLULUKLARI

İSM Bilgi Güvenliği Alt Komisyonu tarafından hazırlanmış Bilgi Güvenliği Yönetim Sistemi Politikasını onaylamak.

Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.

İSM Bilgi Güvenliği Alt Komisyonu tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanan projelere gerekli kaynağı sağlamak.

Çalışmaların yürütülebilmesi için yatırım kararlarına, İstanbul İl Sağlık Müdürlüğü birimlerinde ve üçüncü taraf hizmet alımlarında Bilgi Güvenliği Alt Komisyonu tarafından çalışılan uluslararası standartlar çerçevesinde yapılması gereken çalışma süreçleri, usul ve esaslara dair değişiklikleri onaylamak.

İSM Bilgi Güvenliği Alt Komisyonu tarafından hazırlanmış Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

Belirli aralıklarla yapılacak olan BGYS YGG toplantılarına başkanlık etmek.

Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (yüklenici firma personelleri dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.

Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için İstanbul İl Sağlık Müdürlüğü ve bağlı tüm tesislerde gerekli iç denetimlerin yapılmasına onay vermek.

7. BİLGİ GÜVENLİĞİ ALT KOMİSYON BAŞKANI GÖREV, YETKİ VE SORUMLULUKLARI

İstanbul il Sağlık Müdürlüğü ve bağlı tüm tesislerinde BGYS Politikasının uygulanmasını sağlamak.

Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.

Çalışmaların yürütülebilmesi için gerekli komisyonu oluşturmak ve görev tanımların yapmak.

Bilgi Güvenliği Alt Komisyonuna başkanlık etmek.
İstanbul il Sağlık Müdürlüğü bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standaLlar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, TS ISO/IEC 20000 Bilgi Teknolojileri Hizmet Standardı, Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliklerinin yerine getirilmesi için gerekli çalışmaları onay vermek.
İSM Bilgi Güvenliği Alt Komisyonu tarafından gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
Üst yönetim onayı gerektiren yeni hazırlanan ya da revize edilen dokümanların Üst Yönetim tarafından onaylanmasını sağlamak.

8. BİLGİ GÜVENLİĞİ ALT KOMİSYONU GÖREV, YETKİ VE SORUMLULUKLARI

İSM Bilgi Güvenliği Alt Komisyonu, Bilgi Sistemleri Koordinatörü tarafından oluşturulur, üst yönetim tarafından onaylanır.
Bilgi Güvenliği konularının altyapısını oluşturacak projeleri hazırlamak.
Hazırlanan projelerin gerekliliği olan, birim çalışanlarının ve yüklenici firma personellerinin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm sahaya yayılması için gerekli desteği vermek.
İstanbul il Sağlık Müdürlüğü ve bağlı tüm tesislerinde uygulanması gereken bilgi güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.
Bilgi Güvenliği Alt Komisyon Başkanı tarafından gerekli görüldüğünde toplantılara katılmak.
İstanbul İl Sağlık Müdürlüğü ve bağlı tüm tesislerde Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve Bilgi Sistemleri Koordinatörüne sunmak.
istanbul İl Sağlık Müdürlüğü ve bağlı tüm tesisler ile ilgili yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
İstanbul il Sağlık Müdürlüğü'ne bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standaı1lar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, TS ISO/IEC 20000 Bilgi Teknolojileri Hizmet Standardı gibi standartlar Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliklerinin yerine getirilmesi için proje hazırlamak.
Bilgi Sistemleri Koordinatörü ve Bilgi Güvenliği Yetkilisi ile planlanan ve yürütülen çalışmalara katkı sunmak ve rehberlik etmek.
Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyonların (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi vb.) hazırlanması ve dokümantasyon geliştirme faaliyetlerinde yer almak.
Üst yönetim onayı gerektirmeyen yeni hazırlanan ya da revize edilen BGYS dokümanlarının Bilgi Güvenliği Alt Komisyon Başkanı tarafından onaylanmasını sağlamak.
Projelerin yürütülebilmesi için gerektiğinde, komisyon toplantısı, çalışma grupları toplantısı, konu ile ilgili eğitimler ve bağlı tesislerin ziyareti gibi gerekli organizasyonları yapmak.
İstanbul İl Sağlık Müdürlüğü'ne bağlı tüm tesislerde yapılacak olan çalışmaların proje planlarının

hazırlanması, gerekli bilgilendirme raporları, sunumları ve eğitimlerin organize edilmesi ve gerçekleştirilmesi konularında rehberlik etmek ve katkı sunmak.
Projeler kapsamında yapılacak olan farkındalık eğitimi, temel eğitim, iç denetçi eğitimi gibi konularda gerekli düzenlemeleri ve organizasyonları yapmak.
YGG, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin zamanında ve efektif bir şekilde gerçekleştirilmesi için gerekli planlamaları yapmak.

9. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

9.1. Her yıl İstanbul il Sağlık Müdürlüğü ve bağlı tesislerdeki tüm personellere Bilgi Güvenliği Farkındalık Eğitimleri verilir.

10. POLİTİKA METNİ

İstanbul İl Sağlık Müdürlüğü bilgi güvenliği modeli, Sağlık Bakanllğı 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.

istanbul 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. İlgili taahhütname, https://istanbulism.sağlik.gov.tr/ adresinde yer almaktadır.

İstanbul il Sağlık Müdürlüğü 'ne bağlı tüm tesisler, faaliyetlerini dayanak kısmında belirtilen mevzuat ve başta bu politika olmak üzere üst yönetim tarafından belirlenen bilgi güvenliği politikalarına uygun şekilde yürütmekten sorumludur.

İstanbul il Sağlık Müdürlüğü ve bağlı tesislerdeki tüm personel, https://istanbulism.saglik.gov.tr/ adresinde yayımlanmış olan BGYS politikalarını bilmek ve gerekliliklerini uygulamakla sorumludur.

İstanbul İl Sağlık Müdürlüğü ve bağlı tesislerde herhangi bir bilgi güvenliği ihlal olayı fark edildiğinde, https://bilgiguvenliqi.saglik.gov.tr/Home/OlayBildir adresinde yer alan ihlal bildirimi internet sayfası aracılığı ile bildirilmesi tüm personelin sorumluluğundadır.

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.

Bilişim altyapı hizmetlerine erişmek isteyen (sunucu erişimi, veri tabanı erişimi vb.) dış taraflar mutlak suretle kurum erişim kontrol ve yetki prosedürüne uygun bir şekilde erişim sağlamalıdır. Uygunsuz erişim girişimleri ihlal olayı olarak tanımlanır.

İstanbul il Sağlık Müdürlüğü ve bağlı tesislerde hizmet veren tüm taraflar ile gizlilik sözleşmesi imzalanır.

11. EKLER

Bağlı sağlık **tesisleri** tarafından kullanılacak dokümanlar:

- BG.PO.02 PAROLA YÖNETIMİ POLİTİKASI
- BG.PO.03 E-POSTA KULLANIM POLİTİKASI
- BG.PO.05 ERİŞIM KONTROL POLİTİKASI
- BG.PO.06 YEDEKLEME POLİTİKASI
- BG.PO.07 SOSYAL MÜHENDISLİK ZAFİYETLERİ VE SOSYAL MEDYA GÜVENLIĞİ POLITİKASI
- BG.PR.04 INTERNET VE ELEKTRONİK POSTA KULLANIM PROSEDÜRÜ
- BG.PR.10 UZAKTAN ERİŞİM PROSEDÜRÜ
- BG.FR.07 OLAY BILDIRIM-MÜDAHALE FORMU
- BG.FR.09 AYRICALIKLI ERIŞİM HAKKI TALEP FORMU
- BG.FR.10 DISK İMHA FORMU
- BG.SZ.02 KURUMSAL GIZLILİK SÖZLEŞMESİ
- BG.SZ.01 PERSONEL GIZLILİK SÖZLEŞMESI
- BG.SZ.03 BİLGI GÜVENLİĞİ FARKINDALIK BILDIRGESİ
- BG.SZ.04 UZAKTAN ERIŞİM SÖZLEŞMESI

Bağlı sağlık tesislerinde kurumlara özgü hazırlanması gereken dokümanlar:

- BG.PR.02 BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ PROSEDÜRÜ
- BG.PR.05 GİZLİLİK SÖZLEŞMELERI UYGULAMA PROSEDÜRÜ
- BG.PR.06 KULLANICI HESAPLARININ TANITILMASI, GÖREV DEĞİŞİKLILİĞİ VE İPTAL PROSEDÜRÜ
- BG.PR.09 TAŞINABİLİR ORTAM PROSEDÜRÜ
- BG.PR.11 ERIŞIM KONTROL PROSEDÜRÜ
- BG.PR.12 YEDEKLEME PROSEDÜRÜ
- BG.FR.02 SBYS YETKI DEĞIŞIKLIĞİ FORMU
- BG.FR.03 KABLOSUZ INTERNET ERİŞIMI TALEP FORMU
- BG.FR.04 IŞE BAŞLAMA FORMU
- BG.FR.05 IŞTEN AYRILMA FORMU
- BG.FR.08 YEDEKLEME TESLIM FORMU
- BG.FR.14 YEDEKLEME PLANI
- BG.FR.15 YEDEKLEME KONTROL LİSTESI