1. AMAÇ

Bu politika; Gaziantep İl Sağlık Müdürlüğü ile bağlı tüm birimleri ve 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; Gaziantep İl Sağlık Müdürlüğü, Bağlı birimleri ve 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 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.

- **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.
- **SBSGM:** T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü

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. Bu komisyon ilgili faaliyetleri değerlendirmek üzere 6 (Altı) ayda bir toplanacaktır.

5.2 Bilgi Güvenliği Alt Komisyonu çalışmalarını koordine etmek ve komisyon toplantılarına başkanlık yapmak üzere İSM Destek Hizmetleri Başkanı **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 kılavuzda belirtildiği şekilde **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 bu politikanın 5.6 maddesinde bilgileri verilen personel görevlendirmesi yapılmıştır.

5.6 İSM Bilgi Güvenliği Alt Komisyonu Görevlendirme Tablosu ekte belirtildiği şekildedir.

5.7 İSM Bilgi Güvenliği Alt Komisyonu Organizasyon Şeması

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

5.8.1. İSM BGYS Politikası ve bu politikanın 14.1 maddesinde belirtilen destek dokümanları İSM'ye bağlı tüm birim ve sağlık tesisleri için ortak uygulanır. İSM'ye bağlı Sağlık tesisleri aksi belirtilmedikçe politikalar, formlar, prosedürler, ekler ve belirtilen diğer belgeler üzerinde değişiklik yapamaz, farklı doküman oluşturamaz. İSM ve bağlı tüm sağlık tesislerinde görevli tüm personel bu politikaya ve eklerine uymakla yükümlüdür. Ancak 2. ve 3. Basamak Sağlık Tesisleri İSM tarafından hazırlanan BGYS Politikası ile bu politikanın 3. Maddesinde belirtilen dayanaklara aykırı olmamak şartıyla ve BGYS Alt Komisyonunun bilgisi dahilinde hasta ya da çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması ile ihtiyaç duyulan doğru bilginin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılmasının sağlanması vb konularında İSM BGYS Politikalarına ilişkin BGYS Prosedürü oluşturabilirler.

5.8.2. 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, T.C. Sağlık

Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu A.2.4.3 maddesinde belirtilen niteliklerde bir personel **Bilgi Güvenliği Yetkilisi** olarak görevlendirilir.

5.8.3. İSM'ye bağlı 2 ve 3'üncü basamak sağlık tesislerinde İSM Bilgi Güvenliği Alt Komisyonu ile koordinasyon sağlamak ve benzer görevleri yürütmek üzere Sağlık Tesisi Bilgi Güvenliği Sorumlusuna bağlı olarak bir Hastane Bilgi Güvenliği Ekibinin kurulması sağlık tesisinin sorumluluğundadır. Kurulması halinde bu ekiplerde görev yapan personelin kimlik bilgileri, görev tanımları ve olurları Hastane Hizmet 5.8.3.İSM'ye bağlı 2 ve 3'üncü basamak sağlık tesislerinde İSM Bilgi Güvenliği Alt Komisyonu ile koordinasyon sağlamak ve benzer görevleri yürütmek üzere Sağlık Tesisi Bilgi Güvenliği Sorumlusuna bağlı olarak bir Hastane Bilgi Güvenliği Ekibinin kurulması sağlık tesisinin sorumluluğundadır. Kurulması halinde bu ekiplerde görev yapan personelin kimlik bilgileri, görev tanımları ve olurları Hastane Hizmet Kalite Standartları gereği hazırlanması gereken Hastane Bilgi Yönetim Süreç dokümanlarında belirtilmesi yeterlidir. Bu personele ait bilgilerin ayrıca İl Sağlık Müdürlüğüne gönderilmesine gerek bulunmamaktadır. Kurulması durumunda bu politikaya ve bu politikanın 5.8.1 maddesinde belirtilen açıklama ve dokümanlara aykırı kararlar almamak şartıyla bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat çerçevesinde ve risk değerlendirme metotlarını kullanılarak "Gizlilik, Bütünlük ve Erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;

- Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,
- Bilgi güvenliği ile ilgili tüm yasal mevzuata BGYS kılavuzu çerçevesinde uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- BGYS'yi sürekli gözden geçirmek ve iyileştirilmesi için BGYS sürecine katkıda bulunmak,
- Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler vermek
- Cumhurbaşkanlığı 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" genelgesinde belirtildiği şekilde önlemler almak gibi faaliyetlerde bulunabilir.

5.8.4. İSM'ye bağlı 1 'inci basamak sağlık hizmeti sunumu yapan sağlık teşkillerinde ayrıca bir bilgi güvenliği yetkilisi görevlendirmesi yapılmayacaktır, ilgili kurumda günlük bilgi sistem işletme ve yönetim faaliyetlerini yapmakla sorumlu olan kişi bu politikanın 3. Maddesinde belirtilen dayanaklar ve almış olduğu BGYS farkındalık eğitimleri çerçevesinde 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.

5.8.5. 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. BGYS ÜST YÖNETİM GÖREV, YETKİ VE SORUMLULUKLARI

6.1 Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait Bilgi Sistemleri Koordinatörünü atamak ve yetkilendirmek.

6.2 BGYS Alt Komisyonu tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanmış projelere gerekli kaynağı ve katkıyı sağlamak.

6.3 BGYS Alt Komisyonu tarafından hazırlanmış ve kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.

6.4 BGYS Alt Komisyonu tarafından yapılan görevlendirmelere onay vermek.

6.5 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.

6.6 Belirli aralıklarla yapılacak olan BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.

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

6.8 Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek amacıyla yapılacak olan bağlı birimlere/sağlık tesislerine yönelik iç denetimlerin yapılmasına onay vermek.

6.9 BGYS Alt Komisyonu tarafından hazırlanan ve kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak. Risk iyileştirme planındaki azaltma kararı verilen risklerin kabul edilebilir düzeye getirilebilmesi için gerekli destek ve kaynakları sağlamak, risk iyileştirme planlarını gözden geçirmek, onaylamak ve denetlemek.

6.10 BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynakları sağlamak.

6.11 Kurum Bilgi Güvenliği Taahhütnamesini onaylamak ve web sitesinde herkese açık bir şekilde yayımlanmasını sağlamak.

7. BGYS ALT KOMİSYON BAŞKANI GÖREV, YETKİ VE SORUMLULUKLARI

7.1 İSM BGYS Politikasının İSM ile bağlı birim/sağlık tesislerinde ihtiyaçlar doğrultusunda yasal mevzuat çerçevesinde güncellenmesini ve uygulanmasını sağlamak

7.2 Bilgi Güvenliği konularının altyapısını oluşturacak projelerin hazırlanmasını sağlamak.

7.3 Çalışmaların yürütülebilmesi için gerekli komisyonu oluşturmak ve görev tanımlarını yapmak.

7.4 Bilgi Güvenliği alt Komisyonuna başkanlık etmek ve 6 (Altı) ayda bir toplanmasını sağlamak.

7.5 Bilgi Güvenliği Komisyonundan gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek.

7.6 Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.

8. BGYS ALT KOMİSYONU GÖREV, YETKİ VE SORUMLULUKLARI

8.1 Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını vermek.

8.2 Bilgi güvenliği politikalarının uygulanması, denetlenmesi ve incelenmesi faaliyetlerinde bulunmak.

8.3 Bilgi güvenliği eğitimi ve farkındalığını sağlamak için gerekli planları ve programları hazırlamak, uygulamak ve yönlendirmek.

8.4 İlgili Yönerge ve Kılavuzda belirtilen hususlar çerçevesinde bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlamak.

8.5 Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay sürecini takip etmek.

8.6 BGYS konularını değerlendirmek ve uygulamak amacıyla en az 6 (Altı) ayda bir ya da Bilgi Sistemleri Koordinatörü tarafından gerekli görüldüğü zamanlarda toplanmak.

8.7 BGYS Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay sürecini takip etmek ve bağlı tüm sağlık tesisleri/birimlerde uygulanmasını sağlamak.

8.8 BGYS kapsamında hazırlanan projelerin gerekliliği olan, birim çalışanlarının, danışmanların ve yüklenici firma personelleri ile stajyerlerin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

8.9 Bilgi güvenliği politikası gereği yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılmak, bağlı birim/sağlık tesislerinde bu çalışmaların yayılmasına öncülük etmek, sağlık tesisleri ve birimlere yönelik iyileştirici ve önleyici denetimlerde bulunmak.

8.10 Bakanlık tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlamak.

8.11 Bilgi güvenliği yetkili/yetkililerini belirlemek ve görevlendirmesini yapmak.

8.12 Bakanlık tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde belirtilen esaslar çerçevesinde Kurumsal SOME'sini kurmak ve işletilmesini sağlamak. Kurumsal SOME Ekip Lideri görevlendirmesini yapmak.

8.13 Bilgi güvenliği ekibi ve SOME ekibinin faaliyetlerini denetlemek ve katkıda bulunmak.

9. İL BİLGİ GÜVENLİĞİ YETKİLİSİ GÖREV, YETKİ VE SORUMLULUKLARI

9.1 BGYS Alt Komisyonundan aldığı yetkiye dayanarak SBSGM ile koordineli bir şekilde ve Gaziantep İl Sağlık Müdürlüğü ile bağlı sağlık tesisleri/birimleri bünyesinde bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek.

9.2 BGYS Ana ilkeleri çerçevesinde, SBSGM tarafından verilen eğitimler doğrultusunda BGYS Alt Komisyonunu yönlendirmek ve Gaziantep İl Sağlık Müdürlüğü bağlı birimleri/sağlık tesislerinde bilgi güvenliği ile ilgili konulardaki SBSGM'nin icra organı olarak hareket etmek.

9.3 BGYS Alt komisyonundan aldığı yetkiye dayanarak bilgi güvenliği ile ilgili faaliyetlerinin yürütülmesi kapsamında görev yapan tüm ilgililer ile uygun yöntemlerle iletişim kurmak, bunları yönlendirmek ve BGYS konularında maksimum düzeyde farkındalıklarının artmasını sağlamak

10. BGYS İLKELERİ

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

10.2 Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

10.2.1. Kişisel ve elektronik iletişimde üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,

10.2.2. Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,

10.2.3. Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,

10.2.4. Bilgi güvenliği ihlal olaylarını bu politikanın 11.5 maddesinde belirtildiği adrese belirtildiği şekilde raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.

10.3 Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.

10.4 Kurum bilişim kaynakları, T.C. Yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz.

10.5 Kurumun tüm çalışanları; bu politika ile diğer desteklenen politikalara, prosedürlere, talimatlara, formlara ve sözleşme gerekliliklerine uymakla sorumludur.

10.6 iş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.

10.7 Bilgilerin bütünlüğü her durumda korunacaktır.

10.8 Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.

10.9 Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.

10.10 Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.

10.11 İSM BGYS Politikası kapsamında bulunan tüm gerçek ve tüzel kişiler Bu ilkeler doğrultusunda bu politikaya ve 2019/12 sayılı ve “Bilgi ve İletişim Güvenliği Tedbirleri” konulu Cumhurbaşkanlığı genelgesine uymak zorundadır.

11. BİLGİ HASSASİYETİ VE RİSKLER

a) BİLGİ VARLIKLARIMIZ

T.C. Sağlık Bakanlığı Gaziantep İl Sağlık Müdürlüğü bağlı birimleri/sağlık tesisleri bünyesinde bu politika metninin 2. maddesinde belirtilen kapsam dâhilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları iş ve işlemlerde üretilen bilgiler envantere kayıtlı olup olmadıklarına bakılmaksızın bilgi varlıklarımızın bütünüdür.Masaüstü bilgisayarlar, taşınabilir bilgisayarlar, tabletler, telefonlar, CD, DVD, harici disk ve USB Bellek ortamındaki tüm veriler, evraklar, klasör ve evrak dolapları, sunucular, veri depolama üniteleri vb. gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (İnternet, Email, Telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

b) VARLIKLARIN KATEGORİLERİ

İş Süreçleri: Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas bilgilerin yoğun olarak işlendiği iş süreçleri (yaklaşık maliyet piyasa araştırması, hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.).

Kurumsal Bilgi Varlıkları: Elektronik veya kâğıt ortamda tutulan hasta kayıtları, personel kayıt ve dosyaları, kurumsal evraklar, bilgisayarlarda saklanan ve kurum için değeri olan veriler, raporlar, listeler, çizimler, veri tabanları, veri tabanı yedekleri, faturalar, sözleşmeler, teklifler, telifler, lisanslar vb.

Yazılımlar: İşletim sistemleri, ofis uygulamaları, SBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, EKİP, KPS, HSYS, LBYS vb.) vb.

Fiziksel varlıklar: Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler, CD, DVD vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb),fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar, güvenlik kameraları vb.

Varlık Sahibi: Ek GİS.BG.EK.02'deki Kurum Bilgi Varlıkları Envanter Çizelgesinde varlığın sahibi olarak belirtilen, bu politikanın 11.C maddesinde belirtilen bilgi sınıflandırma kuralları uyarınca, her varlığa bir gizlilik derecesi atayan, gizlilik derecesi yüksek varlıklar için taşıdığı yüksek risk değeri nedeniyle daha sıkı güvenlik tedbirleri uygulayan gerçek bir kişi, bir birim ya da kurumlardır.

Varlık sahipleri, varlıklarını envantere doğru olarak kaydettirmekten, varlıklarına uygun gizlilik derecesi ve varlık değeri atamaktan, varlıklarının uygun şekilde korunmasından, varlıklara erişecek kişi veya süreçleri için erişim izinlerini planlamaktan, bunlarla ilgili kararları vermekten, varlıkların silinmesi ya da imha edilmesinde uygun işlemlerin uygulanmasından ve BGYS Varlık Değeri Tablosunda belirtilen tüm ilkelerin güvenlik hedeflerinin kabul edilebilir düzeye çekilmesi amacıyla yapılan faaliyetlere destek olmak/alınacak tedbirlere uymakla yükümlüdür.

İnsan Kaynakları: Çalışanlar, stajyerler, danışmanlar, hizmet alım personeli, tedarikçi firma personeli, ortak proje paydaşlarıdır. İş akitleri, sözleşmeleri veya anlaşmaları sona erdiğinde, ellerinde olan tüm kurumsal varlıkları iade etmekle mükelleftirler.

Altyapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.

Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

c) VARLIK SINIFLANDIRILMASI

13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren **"Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar"** gereği;

1. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza hayati derecede zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek bilgiler **"çok gizli",**
2. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza büyük zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler **"gizli",**
3. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler **"özel",**
4. İçerdiği bilgi itibarıyla **ÇOK GİZLİ, GİZLİ** veya **ÖZEL** gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgiler **"hizmete özel"** olarak sınıflandırılır.

5.Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişiler tarafından hazırlanıR ve özel usullere göre dağıtımı yapılır. Bu tip evrak ve dokümanlar korumalı odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar İçinde muhafaza edilmelidir.

6. Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilmelidir.
7. Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, **"tasnif dışı"** olarak kabul edilir.
8. Tasnif dışı bir gizlilik derecesi olmayıp, evrakın yukarıda sıralanan gizlilik derecelerinden hiç biri ile sınıflandırılmamış olduğunu belirtir. Tasnif dışı belgeler için herhangi bir erişim kısıtlaması yoktur.
9. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, elektronik ortamda hazırlanması ve dağıtılması ile ilgili hususlar **için Sağlık Bakanlığı Elektronik Belge Yönetim Sistemi Yönergesi'nde** belirtilen kurallar uygulanır.
10. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, kâğıt ortamda hazırlanması ve manuel (elektronik olmayan) yöntemlerle dağıtılması için **Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik** te belirtilen kurallar uygulanır.

11. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından sınıflandırılmaya ihtiyaç duyulan diğer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır. Bu varlıkların korunması ve erişim haklarının düzenlenmesi için alınacak tedbirler, yapılacak olan risk analiz neticesine göre belirlenir.

Sağlık verilerinin korunmasına yönelik risk analizi yapılırken, kişisel verilerin hassasiyeti ve kanuna aykırı bir şekilde ifşası halinde uygulanacak ağır idari ve cezai yaptırımlar nedeniyle en üst düzeyde özen gösterilmelidir.

12. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

a) BGYS EĞİTİMLERİ

İSM ile bağlı birimleri/sağlık tesisleri ve personelin sahip olduğu en değerli varlıkları olan kurumsal ya da kişisel bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Koruma birtakım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilenmesiyle mümkün olabilir.

Güvenliğin en zayıf halkası olarak da kabul edilen insan faktörü üzerinde çeşitli farkındalık programları uygulanması gerekmektedir. Bu programların en başında ise bilgi güvenliği eğitimi yer alır. Kurumumuzda gerekli görüldüğü hallerde görevli tüm personele belirli zaman dilimlerinde aşağıdaki eğitim verilecektir.

b) EĞİTİM İÇERİĞİ

1. Bilgi Güvenliği Yönetim Sistemi Standardı ve Farkındalık Eğitimi
2. Adli Bilişim ve BGYS Hukuksal Boyutu Eğitimi
3. BGYS Siber Güvenlik Eğitimi
4. BGYS Son Kullanıcı Güvenlik Eğitim
5. Sosyal Mühendislik ve Sosyal Medya Farkındalık Eğitimi
6. E-Posta Güvenliği Eğitimi
7. BGYS İhlal Olayları Hakkında Eğitim

13. POLİTİKA METNİ

13.1 Gaziantep İl Sağlık Müdürlüğü bilgi güvenliği modeli bu politikanın 3. DAYANAK maddesinde bulunan yasal mevzuat çerçevesinde, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzuna dayanırve kurumsal bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak için operasyonel ve yönetsel çerçeveyi sunar.

13.2 Gaziantep 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://gaziantepism.saglik.gov.tr** adresinde “Bilgi Güvenliği” menüsünde yer almaktadır.

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

13.4 Tüm personel, **https://gaziantepism.saglik.gov.tr** adresinde "Bilgi Güvenliği" menüsünde yayımlanmış olan BGYS politikalarını bilmek ve gerekliliklerini uygulamakla sorumludur. Aksi şekilde davranan personel hakkında ağır idari ve cezai yaptırımlar uygulanır.

13.5 Bilgi güvenliği ihlal olayı fark edildiğinde, İSM tarafından bağlı birim ve sağlık tesislerine gönderilen 0080529233 barkod numaralı, 09/11/2018 tarihli ve "Bilgi Güvenliği İhlal Olayları Hk." konulu resmi yazıda belirtilen açıklama ve tedbirler doğrultusunda https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan ihlal bildiriminin internet sayfası aracılığı ile bildirilmesi tüm personelin sorumluluğundadır.

13.6 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.

13.7 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.

13.8 İl Sağlık Müdürlüğü ile bağlı sağlık tesislerine bilgi güvenliği politikası kapsamında hizmet veren tüm taraflar ile gizlilik sözleşmesi imzalanır.

14. EKLER

14.1 Tüm Sağlık Teşkilleri Tarafından Ortak Olarak Kullanılacak Destek Dokümanları

- İSM BİLGİ GÜVENLİĞİ ORGANİZASYONDA GÖREV YAPAN PERSONEL BİLGİLERİ
- GİS.BG.PO.02 E-POSTA KULLANIM POLİTİKASI
- GİS.BG.PO.04 PAROLA YÖNETİMİ POLİTİKASI
- GİS.BG.PO.05 PAROLA GÜVENLİĞİ POLİTİKASI
- GİS.BG.PO.06 ERİŞİM KONTROL POLİTİKASI
- GİS.BG.PO.07 YEDEKLEME POLİTİKASI
- GİS.BG.PO.08 MAL VE HİZMET ALIMI GÜVENLİĞİ POLİTİKASI
- GİS.BG.PO.09 SOSYAL MÜHENDİSLİK ZAFİYETLERİNE KARŞI ALINACAK ÖNLEMLER VE SOSYAL MEDYA GÜVENLİĞİ POLİTİKASI
- GİS.BG.PR.01 BİLGİ GÜVENLİĞİ DİSİPLİN PROSEDÜRÜ
- GİS.BG.PR.02 BİLGİ GÜVENLİĞİ İHLAL OLAYLARI PROSEDÜRÜ
- GİS.BG.PR.07 İNTERNET VE ELEKTRONİK POSTA PROSEDÜRÜ
- GİS.BG.PR.09 TAŞINABİLİR ORTAM PROSEDÜRÜ

- GİS.BG.PR.10 UZAKTAN ERİŞİM PROSEDÜRÜ
- GİS.BG.FR.10 AYRICALIKLI ERİŞİM HAKKI TALEP FORMU
- GİS.BG.PR.11 GÜVENLİ VERİ SİLME PROSEDÜRÜ
- GİS.BG.SZ.01 PERSONEL GİZLİLİK SÖZLEŞMESİ
- GİS.BG.SZ.02 KURUMSAL GİZLİLİK TAAHHÜTNAMESİ
- GİS.BG.SZ.03 BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ
- GİS.BG.SZ.04 UZAKTAN ERİŞİM SÖZLEŞMESİ
- GİS.BG.EK.05 AİLE HEKİMLERİ İÇİN E-NABIZ ERİŞİM İŞ AKIŞI
- GİS.BG.EK.06 SAĞLIK TESİSİ HEKİMLERİ İÇİN E-NABIZ ERİŞİM İŞ AKIŞI
- MERNIS TAAHHÜTNAMESİ

14.2 Sağlık Teşkilleri Tarafından Kendi Kurumlarına Özgü Hazırlanması Gereken Destek Dokümanları

- FİZİKSEL VE ÇEVRESEL GÜVENLİK PROSEDÜRÜ
- BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ PROSEDÜRÜ
- KULLANICI HESAPLARININ TANITILMASI, GÖREV DEĞİŞİKLİLİĞİ VE İPTAL PROSEDÜRÜ
- GİZLİLİK SÖZLEŞMELERİ UYGULAMA PROSEDÜRÜ
- ERİŞİM KONTROL PROSEDÜRÜ VE ERİŞİM KONTROL MATRİSLERİ
- VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ
- TEMİZ MASA TEMİZ EKRAN POLİTİKASI
- YEDEKLEME PLANI
- YEDEKLEME KONTROL LİSTESİ
- YEDEKLEME TESLİM FORMU
- YEDEKLEME PROSEDÜRÜ
- BGYS VARLIK DEĞERİ TABLOSU
- İŞE BAŞLAMA, GÖREV DEĞİŞİKLİĞİ VE İŞTEN AYRILMA PROSEDÜRÜ
- SİSTEM GÜVENLİK PROSEDÜRÜ