1. **AMAÇ**

Samsun Ruh Sağlığı ve Hastalıkları Hastanesi bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, uyulması gereken kuralları içeren bir dokümandır.

Samsun Ruh Sağlığı ve Hastalıkları Hastanesine ait mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içerisinde derlenen tüm bilgiler ile hastalarımızın teşhis ve tedavilerinin desteklenmesi ve sürdürülmesi için gerekli her türlü verinin bütünlüğünün sağlanması, bunların yasal mevzuata uygun sürelerle saklanması, teşhis ve tedaviyi yürütecek tıbbi ekip dışında 3. kişilerle paylaşılmasının önlenmesi amaçlanmaktadır

**2.KAPSAM**

Samsun Ruh Sağlığı ve Hastalıkları Hastanesi ve tüm bağlı birimleri kapsar. Bilgi Güvenliği Politikası aşağıdaki varlık ve teknoloji kategorilerini ;

* Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
* Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,
* Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, uydu 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 varlıkları,
* Kurum tarafından üretilen, kullanılan ve/veya geliştirilen tüm verileri kapsar.

**3. TANIMLAR ve KISALTMALAR**

**BGYS:** Bilgi Güvenliği Yönetim Sistemi

**BTHYS:** Bilgi Teknolojileri Hizmet Yönetim Standardı

**Bilgi Güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirdik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

**Bilgi güvenliği ihlal olayı:** İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

**Bilgi güvenliği yönetim sistemi (BGYS) :** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, işleyişi ve kaynakları içerir.

**Bilgi Güvenliği Riski:** Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür.

**Risk Yönetimi:** Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.

**Risk Analizi:** Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması.

**Risk Değerlendirme:** Risk analizi sonucu bulunan değerlerin yorumlanması ve derecelendirilmesi.

**Riskin Kabulü/Kabul edilebilir Risk:** Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme.

Riskten Kaçınma: Riski oluşturan durumdan kaçınma.

**Risk İletimi:** Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.

**Riski Belirleme:** Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerin belirlenmesini içeren süreçtir.

**Komisyon Toplantıları:** Her üç ayda ve ihtiyaç halinde toplantılar yapılarak gerekli analizler ve iyileştirme faaliyetleri planlanır.

**4.** **BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ**

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır.

Bilgi diğer kıymetli varlıklarımızın içinde kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sisteminizde varlıklarımız tespit edilmiş, riskler belirlenmiş, aylık analizler ve gerekli değerlendirmeler yapılarak süreç takibi yapılmaktadır.

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.

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.

Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

1. **BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU**

**BGYS TAKIMI VE YETKİLERİ**

Sağlık Bakanlığı Samsun İl Sağlık Müdürlüğü Samsun Ruh Sağlığı ve Hastalıkları Hastanesi bünyesinde bu politika metninde tarif edilen kapsam dâhilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS Komisyonu, BGYS Çalışma Grubu ve Bilişim Teknik Destek Alt Çalışma Grubu kurulmuştur,

**Bilgi Güvenliği Üst Yönetim Görev, Yetki Ve Sorumluluklar:**

* Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.
* Bilgi güvenliği yetkilisi ve/veya çalışma grubu tarafından hazırlanmış komisyon tarafından onay verilmiş bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için hazırlanan faaliyetlere gerekli kaynağı sağlamak.
* BGYS yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.
* BGYS yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.
* Belirli aralıklarla yapılacak olan komisyon toplantılarına başkanlık etmek.
* Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (firma personeli 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 gerekli iç denetimlerin yapılmasına onay vermek.
* BGYS yetkilisi tarafından hazırlanmış, BGYS Komisyonu tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

***BGYS Komisyon Başkanı Görev, Yetki ve Sorumlulukları:***

* Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.
* Çalışmaların yürütülebilmesi için gerekli komisyonları, çalışma gruplarını oluşturmak ve görev tanımlarını yapmak.
* BGYS Komisyonuna başkanlık etmektir.
* BGYS Biriminden, BGYS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek faaliyetlerin dayandırıldığı standartlar çerçevesinde onay vermek.
* Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
* Yapılan çalışmalarla ilgili üst yönetime ve BGYS Komisyonuna rapor sunmak ve bilgilendirme toplantıları düzenlemek.

***BGYS Yetkilisi Görev ve Sorumlulukları:***

* Bilgi Güvenliği altyapısının oluşturulmasını sağlamak.
* Samsun Ruh Sağlığı ve Hastalıkları Hastanesinde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve çalışma grubuna katkı sunmak.
* Samsun Ruh Sağlığı ve Hastalıkları Hastanesinde yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
* Ruh Sağlığı ve Hastalıkları Hastanesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde bir hizmet kalitesi sunulmasını sağlamak.
* BGYS Üst Yönetim, Komisyon ve Çalışma Grubu ile planlanan ve yürütülen çalışmalara katkı sunmak ve rehberlik etmek.
* Ruh Sağlığı ve Hastalıkları Hastanesinde yapılacak olan çalışmaların proje planlarının hazırlanması, gerekli bilgilendirme raporları, sunumları ve eğitimlerin organize edilmesi ve gerçekleştirilmesi konularında rehberlik etmek ve katkı sunmak.

***BGYS Komisyonu Görev, Yetki ve Sorumluluklar:***

* BGYS Komisyonu BGYS Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.
* BGYS Yönetim Temsilcisi bu komisyona başkanlık eder.
* BGYS yönetim temsilcisi ve BGYS yetkilisi tarafından gerekli görüldüğünde toplantılara katılmak.

Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.

* Hastane içinde bilgi güvenliği ihlali ya da tehdidi olabilecek durumları toplantılara gündem maddesi olarak taşımak

***BGYS Çalışma Grubu, Yetki ve Sorumluluklar:***

* BGYS çalışma grupları BGYS Yönetim Temsilcisi tarafından oluşturulur, BGYS Komisyonu kabul eder ve üst yönetim onaylar.
* BGYS Yetkilisi ve Yönetim Temsilcisi tarafından planlanan çalışmalara katılmak.
* BGYS Yetkilisine ve Yönetim temsilcisine karşı sorumludurlar.
* Planlanan çalışmalara BGYS Yetkilisi, BGYS Yönetim Temsilcisi istekleri paralelinde katkı sunmak.
* Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılmak bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük etmek.

***BGYS TOPLANTILARI***

* Yıllık olarak hazırlanan komisyon toplantıları planları olup işleyişin ve bilgi güvenliği süreçlerinin değerlendirildiği toplantılardır. Başlatılan düzeltici ve önleyici faaliyetlerden OLUMSUZ Kapatılanlar yılda bir kez yapılan hastane üst yönetim toplantılarına taşınmasıdır.
* Bu toplantılarda standarda göre girdi ve çıktılar Toplantı Tutanağı Formu kullanılarak kayıt altına alınmaktadır.

**6.BİLGİ HASSASİYETİ VE RİSKLER**

**6.1.Bilgi Varlıklarımız**

T.C. Sağlık Bakanlığı Samsun İl Sağlık Müdürlüğü Samsun Ruh Sağlığı ve Hastalıkları Hastanesi bünyesinde Madde 2 de belirtilen kapsam dâhilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

**6.2.Varlık Sınıflandırılması**

|  |  |  |
| --- | --- | --- |
| **BİLGİ SINIFLANDIRMA KILAVUZU** | | **Saklanma Yeri Dolap** |
| **Gizli** | En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır. | Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar |
| **İç Kullanım** | Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır. | Departmanın kilitli dolapları, kişisel bilgisayarlar |
| **Kişisel** | Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır. | Çalışma masalarının kilitli çekmeceleri |
| **Kuruma Açık** | Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer. | Departmanın kilitli ortak dolapları |
| **Halka Açık** | Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir. | Dolaplar ve dolap dışlarında |

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kâğıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

**Bilgi Güvenliği Politika, Prosedür Ve Kılavuzu**

BGYS Politikası kurumumuzca yayınlanan bir çok farklı politika, prosedür, talimat ve rehberi kontrol ve risk yönetimi amaçları çerçevesinde adresler.

**Bilgi Güvenliği Politikası ve Kılavuzu**

T.C. Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Yönergesi ve kılavuzu çerçevesinde, Samsun Ruh Sağlığı ve Hastalıkları Hastanesi tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

**Bilgi Güvenliği Prosedürleri ve Politikaları**

Bilgi yedekleme, ihlal olayı müdahale, iç denetim, doküman ve kayıtların kontrolü, kullanıcı tanımlama, acil durum eylem planı, sistemin işleyişi anlatılmaktadır. İlgili çalışanlar yönetimce tanımlanan ve yayınlanan bu prosedür ve politikalara uygun hareket etmelidirler.

**Bilgi Güvenliği Sözleşmeleri**

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) kurum personelleri (657-4c-4b vs) ile personel çalıştırılmasına dayalı olan veya olmayan hizmet yapım ve mal alımları ile işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

**Bilgi Güvenliği Eğitimleri**

Samsun İl Sağlık Müdürlüğü Samsun Ruh Sağlığı ve Hastalıkları Hastanesi bünyesinde çalışan tüm personele Bilgi Güvenliği Farkındalık Eğitimi yılda en az bir defa verilecek olup sağlık tesislerimizin hizmet içi eğitim planlarına dahil edilmiştir.

**7.POLİTİKANIN İHLALİ VE YAPTIRIMLAR**

Bilgilerin gizli tutulması yükümlülüğü, gizlilik ve mahremiyeti sözleşmesinin ihlali durumunda izlenecek yasal süreç

1. Bilgiye erişim yetkisi olan personellerin ulaşmış oldukları bilgileri gizli tutma yükümlülüğü olup, kişilerin kurumla yaptıkları personel gizlilik sözleşmesi gereği bu bilgileri ifşa edemezler.

2. Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, 657 sayılı Devlet Memurları kanunun 125 Maddesinde yer alan hükümler uygulanacaktır.

3. 657 sayılı Devlet Memurları Kanun hükümlerine tabi olmayan personelin (Danışmanlar, Firma Personelleri) kurumla aralarındaki sözleşmelerde yer alan hükümler uygulanacaktır aksi durumda genel hukuk kurallarına tabi olacaktır.

4. 657sayılı Devlet Memurları Kanunda yer alan ve diğer kabul edilecek cezai yaptırımlar aşağıdaki gibi olacaktır.

a. Uyarma,

b. Kınama,

c. Aylıktan kesme,

d. Kademe ilerlemesinin durdurulması,

e. Devlet Memurluğunda çıkarma,

f. Para cezası (657 dışında kalanlarla yapılan sözleşmeler gereği),

g. Sözleşme feshi.

h. Dava edilmesi

**8.POLİTİKANIN YÜRÜRLÜĞE GİRİŞİ**

Politikanın yayınlanma tarihinden itibaren hastane yöneticisinin onayıyla yürürlüğe girer.

**9.POLİTİKANIN DUYURULMASI**

İşbu "**Bilgi Güveliği Politikası**" yürürlüğe girmesinin ardından Tüm çalışanların dokümana ulaşma şansı sağlanmıştır. Kurum Web sitesine eklenir. Politikanın tüm personelce okunup okunmadığı sağlık tesisinin yöneticisinin sorumluluğundadır.

**10.POLİTİKANIN GÖZDEN GEÇİRİLMESİ**

Bilgi Güvenliği Politikası, Bilgi Güvenliği Sorumluları tarafından periyodik olarak altı ayda bir gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Kurum Yönetimi tarafından onaylanır. Onaylanan politika Kurum internet sitesinde yayımlanır.

**Uzm. Dr. Asibe ÖZCAN**

**Başhekim**