BGYS politikası, T.C. Sağlık Bakanlığı Gercüş Devlet Hastanesi 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.

1. AMAÇ

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 yönetim sistemimiz TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde **PUKÖ** (Planla, Uygula, Kontrol Et, Önlem Al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır.

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. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

2. KAPSAM

Bu politika, Kurum Bilgi Sistemleri alt yapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet ,yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. TANIMLAR ve KISALTMALAR

a. **BGYS**: Bilgi Güvenliği Yönetim Sistemi
b. **BTHYS:** Bilgi Teknolojileri Hizmet Yönetim Standardı
c. **Risk Yönetimi:** Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.
d. **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.
e. **Risk Değerlendirme:** Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesi.
f. **Risk İşleme:** Risk değerlendirme sonuçlarına bağlı olarak kaçınma, kabul, kontrol, transfer seçeneklerinden birinin seçilmesi ve uygulama planı.

g. **Artık Risk:** Risklerin işlemeden sonra kalan miktarıdır.
h. **Risk Derecelendirmesi:** Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması sürecidir.
i. **Riskin Kabulü/Kabul edilebilir Risk**: Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme.
j. **Bilgi Güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.
k. **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.
l. **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, prosesleri ve kaynakları içerir.
m. **Uygulanabilirlik Bildirgesi (SOA-Statement of Applicability):** Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir. Kontrol amaçları ve kontroller, risk

n. değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.
o. **Etki:** İş hedeflerinin başarısını etkileyen değişim.
p. **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.
q. **Riskten kaçınma:** Riski oluşturan durumdan kaçınma kararıdır.
r. **Risk iletimi:** Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.
s. **Riski belirleme:** Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerinin belirlenmesini içeren süreçtir.
t. **Riski transfer etme:** Bir riskin kayıplarını diğer paydaşlarla paylaşma. (Sigorta yaptırma gibi)
u. **YGG:** Yönetimin Gözden Geçirilmesi
v. **PUKÖ**: Planla, Uygula, Kontrol Et, Önlem Al
w. **EYS**: Entegre Yönetim Sistemi

4. 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.

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

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

5.1. BGYS TAKIMI VE YETKİLERİ

Sağlık Bakanlığı (kurum adı yazılacak) bünyesinde bu politika metninde madde 1.2 de tarif edilen kapsam dahilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS KOMİSYONU ve BGYS ÇALIŞMA GRUPLARI kurulmuştur.

BGYS KOMİSYONU

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KOMİSYON EKİBİ GÖREVLENDİRİLEN PERSONEL LİSTESİ			
S.NO	**ADI SOYADI**	**Ünvanı**	**Yedek Üye**
1	Ayhan IŞIK (Başkan)	Başhekim	H.Siraç TÜREN
2	H.Siraç TÜREN (Üye)	İdari Mali İşler Müdürü	Sadrettin KÖLGE
3	Sadrettin KÖLGE (Üye)	Sağlık Bakım Hizmetleri Müd.	Yusuf Durmuş
4	Yusuf DURMUŞ (Üye)	Kalite Direktörü	Selahat ARSLAN
5	Cahid ATILĞAN (Üye)	Bilgi İşlem Sorumlusu	Fethullah BARLAK
6	Tevfik ÖNER (SOME) (Üye)	Bilgi İşlem Personeli	Hüseyin ÖZMEN
7	Rıdvan YILDIZ (SOME) (Üye)	Mutemet	İbrahim Halil Mutlu

BGYS ÇALIŞMA GRUBU

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ ÇALIŞMA GRUBU GÖREVLENDİRİLEN PERSONEL LİSTESİ			
S.NO	**ADI SOYADI**	**Ünvanı**	**Yedek Üye**
1	H.Siraç TÜREN (Başkan)	İdari Mali İşler Müdürü	Sadrettin KÖLGE
2	Sadrettin KÖLGE (Üye)	Sağlık Bakım Hizmetleri Müd.	Şeyma Nur ODACI
3	Yusuf DURMUŞ (Üye)	Kalite Direktörü	Esma ATILĞAN
4	Cahid ATILĞAN (Üye)	Bilgi İşlem Sorumlusu	Fethullah BARLAK
5	Tevfik ÖNER (Üye)	Bilgi İşlem Personeli	İbrahim Halil MUTLU
6	Rıdvan YILDIZ (Üye)	Mutemet	İsmail GÜNEŞ
7	Selahat ARSLAN (Üye)	Personel Birimi	Fırat DEMİR

ORGANİZASYON ŞEMASI

BG Üst Yönetim Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.
- 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.
- BGYS Birimi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.
- BGYS Birimi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.
- Çalışmaların yürütülebilmesi için yatırım kararlarına, Genel Müdürlük Birimlerinde ve üçüncü taraf hizmet alımlarında BGYS birimi tarafından çalışılan uluslararası standartlar çerçevesinde yapılması gereken çalışma süreçleri, usul ve esaslara dair değişiklikleri onaylamak.
- Belirli aralıklarla yapılacak olan BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.
- 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.

- Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.
- BGYS Birimi 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.

- Gercüş Devlet Hastanesi bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar 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 yapmak.
- BGYS Biriminden, BGYS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
- Projelerde referans alınan standartların temel gereksinimlerinden olan Bilgi Güvenliği Yönetim Sistemi gerekliliklerini oluşturmak ve yönetmek.
- Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
- Çalışmaların yürütülebilmesi için T.C. Sağlık Bakanlığı Genel Müdürlükleri ve diğer birimleri ile taşra teşkilatı ve yüklenici firmalara yönelik gerekli tüm resmi yazışmaların yapılmasını, izinlerin alınmasını sağlamak ve onaylamak.
- Projelerin yürütülebilmesi için gerekli olan yönetim hizmetleri çerçevesinde ihtiyaçların temin edilmesinin sağlanması.
- T.C. Sağlık Bakanlığına bağlı birimlerde ve taşra teşkilatlarında yürütülecek olan uluslararası düzeyde belgelendirme faaliyetlerinin işlerliğini gözden geçirmek için gerekli denetim ekiplerini oluşturmak ve denetimlerin yapılmasını sağlamak.
- Yapılan çalışmalarla ilgili üst yönetime ve BGYS Komisyonuna rapor sunmak ve bilgilendirme toplantıları düzenlemek.
- Yönetim sistemi gerekliliklerinden olan Yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin gerçekleşmesini sağlamak.
- Yapılan çalışmalar doğrultusunda yapılacak olan belgelendirme dış denetimlerini (Belgelendirme ve ara denetimler) organize etmek.
- Projelerin daha verimli bir şekilde yürütülebilmesi için BGYS Birim personelinin kişisel gelişimleri için gerekli görülen eğitimleri düzenlemek ya da dış taraflarda düzenlenmiş eğitimlere gönderilmesini sağlamak konu ile ilgili tüm yasal izin ve finansal kaynağın sağlanmasını organize etmek.

BGYS Birimi Görev, Yetki ve Sorumlulukları

- Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.
- T.C. Sağlık Bakanlığına bağlı diğer birimlerde ve tüm taşra teşkilatında uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve Proje Teknik Sorumlusu & Koordinatöre katkı sunmak.
- T.C. Sağlık Bakanlığına bağlı diğer birimlerde ve tüm taşra teşkilatı ile ilgili yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
- Gercüş Devlet Hastanesi bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar 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 yapılan çalışmalara katkı sunmak.
- BGYS Yönetim Temsilcisi ve Proje Sorumlusu & Koordinatörü ile planlanan ve yürütülen çalışmalara katkı sunmak ve rehberlik etmek.
- Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerine katılmak, dokümantasyon geliştirme faaliyetlerinde yer almak.
- Hazırlanan dokümantasyonun yönetim temsilcisi ve (gerekli olanların) üst yönetim tarafından onaylanmasını sağlamak.
- 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.
- T.C. Sağlık bakanlığına 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.

- 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.
- 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.
- Yönetim sistemi gerekliliklerinden olan Yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin zamanında ve efektif bir şekilde gerçekleştirilmesi için gerekli planlamaların gerçekleşmesini sağlamak.

BGYS Komisyonu Görev, Yetki ve Sorumluluklar:

- BGYS Komisyonu BGYS Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.
- BGYS Yönetim Temsilcisi bu komisyona başkanlık eder.
- Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek.
- 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.
- Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.
- 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.

BGYS Çalışma Grubu, Yetki ve Sorumluluklar:

-BGYS çalışma grupları BGYS Yönetim Temsilcisi tarafından oluşturulur, BGYS Komisyonu kabul eder ve üst yönetim onaylar.

-BGYS birimi ve Yönetim Temsilcisi tarafından planlanan çalışmalara katılmak.

-BGYS birimine ve Yönetim temsilcisine karşı sorumludurlar.

- Planlanan çalışmalara BGYS Birimi, BGYS Yönetim Temsilcisi istekleri paralelinde katkı sunmak.

- Çalışma Grubu Başkanı yapılacak çalışmalarla ilgili gerekli gördüğünde Değerlendirme toplantılarını düzenler.
- Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılmak bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük etmek.

BGYS Forumu Görev, Yetki ve Sorumlulukları

- Forum üyeleri BGYS Birimi, BGYS komisyonu ve Çalışma grubu üyelerinden oluşur.
- Yürütülen çalışmalarla ilgili görüş bildirmek için gönderilen dokümanlara ve e-maillere en kısa sürede cevap vermek.
- BGYS Forumu sistem birimi tarafından teknik bir personel ile BGYS Birimi Projeler Sorumlusu & Koordinatör tarafından yönetilir.

BGYS YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNETİM GÖZDEN GEÇİRME)TOPLANTILARI

BGYS biriminin ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve önleyici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler.

Bu toplantılarda standarda göre girdi ve çıktılar **Toplantı Tutanağı Formu** kullanılarak kayıt altına alınmaktadır.

6. RİSK YÖNETİMİ

6.1. Risk Analizi ve Yönetim Stratejisi

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetle ilgili kayıtlar risk değerlendirme raporunda tutulmaktadır. Kapsam dahilinde ki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Varlık envanteri ile her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır.

Risk analizi çalışması Tehdit Olasılığı ve İşe etkisi boyutlarında değerlendirilecektir. Risk hesaplama formülü kullanılarak her bir varlık için var olan risk değeri hesaplanır. Risk takip tablosunda tanımlanan her bir risk için 6 aylık risk durum değerlendirmeleri yapılarak son durum hesaplanır. Risk değerleri için Risk Değerlerine Göre İşleme Seçeneklerinden uygun olanı seçilir. Kontroller ISO 27001:2005'in Ek-A maddesinden seçilerek uygun olanlar her bir riske atfedilir. Kontrolün nasıl uygulanacağı, kim tarafından uygulanacağı Risk İşleme Takip Tablosunda izlenir. 6 Aylık periyotlarla risk işleme faaliyetlerinin durumu varlık sahiplerinin de katıldığı BGYS komisyonunda değerlendirilir.

6.4.SOA - Uygulanabilir

Risk işleme seçenekleri standardın EK-A bölümünde verilen A.5'den A.15'e 11 kontrol ailesi, 39 farklı başlık ve 133 farklı kontrol olarak verilen listeden seçilebilir. Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı SOA (Statement of Applicability) olan dokümanda belirtilmektedir. SOA Gizli bilgi sınıfındadır. BGYS biriminin ve BGYS Komisyonunun erişimine açıktır.

Bilgi güvenliği amaçları ve uygulamaları SOA'da detaylandırılmıştır. Risk İşleme planı ve SOA paralel dokümanlardır. Risk işleme planında seçilen kontrollerin isimleri veya EK-A'dan seçilmişlerse A.X.X şeklinde kontrol numarasına atıf yapılırken SOA'da kontroller detaylandırılmıştır. Uygulanan ve uygulanacak tüm kontroller SOA'da kaydedilir. Bu doküman risk işleme planı ile bir çapraz kontrol sağlayarak herhangi bir kontrolün atlanmamasını sağlamaktadır.

7. Bilgi hassasiyeti ve riskler

7.1. Bilgi Varlıklarımız

T.C. Sağlık Bakanlığı (kurum adı yazılacak) bünyesinde Madde 1.2 de belirtilen kapsam dahilinde 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, email, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

7.2. 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
Kurıma 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 kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

7.3. Kritik varlıklar

Varlık Kritik Değer Tablosundaki 7 - 11 arası varlıklar kritik varlık olarak kabul edilecektir. Bu varlıklar risk değerlendirme tablosundan faydalanılarak oluşturulacaktır

8. 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.

8.1. Bilgi Güvenliği Politikası ve Kılavuzu

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

8.2. Bilgi Güvenliği Prosedürleri ve Planları

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

8.3. Bilgi Güvenliği Kitapçığı

Kurum bünyesinde tüm çalışanların genel olarak uyması gereken kurallar kitapçık olarak hazırlanıp tüm personele dağıtılmıştır. Personel bu kitapçıkta önerilen uygulamaları takip etmeli, zayıflık ve tehditlere karşı farkında olmalıdırlar. Personel bu kitapçıkta tanımlanan bilgi güvenliği ihlallerini yapmamalı ve bu ihlalleri gözlemlediğinde mutlaka BGYS birimine bildirmelidirler.

8.4. 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) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

9. Bilgi Güvenliği Eğitimleri

Bilgi güvenliği eğitimlerimiz Yıllık eğitim planında belirlenmiş olup düzenli olarak eğitimler verilmektedir.

10. Doküman ve Kayıtların Kontrolü

BGYS ile ilgili dokümanların hazırlanması, yayınlanmadan önce onaylanması, değişikliklerinin revizyonlarının takibi, gerekli noktalarda doğru versiyonun ulaşılabilir olması amaçlarını yerine getirecek **Doküman Hazırlama ve Kodlama Prosedürü** hazırlanmıştır. Dokümanların kontrolü bu prosedüre uygun olarak yapılmaktadır.

Kayıtların kontrolü, saklanması, yedeklenmesi, gerektiğinde tekrar elde edilebilmesini sağlamak amacıyla **Kayıtların Kontrolü Prosedürü** hazırlanmış ve uygulanmaktadır

Bilgi Güvenliği İç Denetimler.

11. Bilgi Güvenliği İç Denetimler.

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği **İç Tetkik Prosedüründe** tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir

12. Sürekli İyileştirme ve Düzeltici – Önleyici Faaliyetler

İç tetkiklerde, ihlal olaylarıyla veya personelin kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların henüz ortaya çıkmadan önce nasıl önleneceğine ilişkin **Düzeltici ve Önleyici Faaliyetler Prosedürü** hazırlanmış ve uygulanmaktadır. Tüm personel düzeltici ve önleyici faaliyetlere katılmakla sorumludur.