BGYS POLİTİKASI

BGYS politikası, T.C. Sağlık Bakanlığı Türkiye Kamu Hastaneleri Kurumu Samsun Gazi 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

Gazi Devlet Hastanesi'ne 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. 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

Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesi ve tüm bağlı birimleri kapsar. Bilgi Güvenliği Planı aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır:

- 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.

2. 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, açıklanabilirlik, 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, prosesleri 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.

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

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.

YGG: Yönetimin Gözden Geçirilmesi

PUKÖ: Planla, Uygula, Kontrol Et, Önlem Al

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

BGYS TAKIMI VE YETKİLERİ

Sağlık Bakanlığı Türkiye Kamu Hastaneleri Kurumu Samsun Gazi Devlet Hastanesi bünyesinde bu politika metninde tarif edilen kapsam dahilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere Bilgi Güvenliği Komisyonu ve Bilgi Güvenliği Çalışma Grubu kurulmuştur. Oluşturulan komisyon ve çalışma grupları hastane yönetimi tarafından görevlendirilme yapılarak belirlenmektedir.

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 projelere gerekli kaynağı sağlamak.
- Bilgi Güvenliği yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.
- Bilgi Güvenliği yetkilisi tarafından hazırlanmış, BGYS komisyonu tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.
- 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 (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.
- Bilgi Güvenliği yetkilisi tarafından hazırlanmış, Bilgi Güvenliği Komisyonu tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

Bilgi Güvenliği 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.
- Bilgi Güvenliği Komisyonuna başkanlık etmektir.
- Bilgi Güvenliği Biriminden, BGYS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek Projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
- Bilgi Güvenliği YS Biriminden, BG Bilgi Güvenliği YS Komisyonundan ve Çalışma Grubundan gelen istek ve talepleri değerlendirmek Projelerin dayandırıldığı standartlar çerçevesinde onay vermek.

- Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
- Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.
- Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.
- Projelerin yürütülebilmesi için gerekli olan yönetim hizmetleri çerçevesinde ihtiyaçların temin edilmesinin sağlanması.
- 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.

Bilgi Güvenliği Yetkilisi Görev ve Sorumlulukları:

- Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.
- Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesine bağlı birimlerde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve çalışma grubuna katkı sunmak.
- Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesine bağlı birimlerde yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
- Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesine bağlı birimlerde 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 yapılan çalışmalara katkı sunmak.
- Bilgi Güvenliği Üst Yönetim, Komisyon ve Çalışma Grubu 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, birim ziyaretleri gibi çalışmaların organize edilmesi, yasal izinlerin, araç izinlerinin alınması gibi hususlarda gerekli organizasyonları yapar.
- Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesine bağlı birimlerde 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, 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.

Bilgi Güvenliği Komisyonu Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği Komisyonu Bilgi Güvenliği Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.
- Bilgi Güvenliği Yönetim Temsilcisi bu komisyona başkanlık eder.
- Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek.
- Samsun Kamu Hastaneleri Birliği Genel Sekreterliğine bağlı sağlık tesislerinde Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.
- Bilgi Güvenliği yönetim temsilcisi ve Bilgi Güvenliği yetkilisi tarafından gerekli görüldüğünde toplantılara katılmak.
- Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.

Bilgi Güvenliği Çalışma Grubu, Yetki ve Sorumluluklar:

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

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

Bilgi Güvenliği 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. Bilgi hassasiyeti ve riskler

6.1.Bilgi Varlıklarımız

T.C. Sağlık Bakanlığı Türkiye Kamu Hastaneleri Kurumu Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesi 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.

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

7. Bilgi Güvenliği Politika, Prosedür Ve Kılavuzu

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

7.1.Bilgi Güvenliği Politikası ve Kılavuzu

T.C. Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Yönergesi ve kılavuzu çerçevesinde, Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesi tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

7.2.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.

7.3 Bilgi Güvenliği Kitapçığı

Kurum bünyesinde tüm çalışanların uyması gereken kurallar kitapçık olarak hazırlanıp tüm personele dağıtılmıştır. Ayrıca bu kitapçık doküman halinde online eğitim modülene yüklenmiştir. Personel bu kitapçıkta önerilen uygulamaları takip etmeli, zayıflık ve tehditlere karşı farkında olmalıdır. Personel bu kitapta tanımlanan bilgi güvenliği ihlallerini yapmamalı ve bu ihlaller gözlemlendiğinde mutlaka Bilgi Güvenliği birimine bildirmelidir.

7.4 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) 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.

8. Bilgi Güvenliği Eğitimleri

Samsun Kamu Hastaneleri Birliği Gazi Devlet Hastanesi bünyesinde çalışan tüm personele Bilgi Güvenliği Farkındalık Eğitimi verilmekte olup, Bağlı Sağlık Tesislerinin hizmet içi eğitim planlarına dahil edilmiştir.

9. PLANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği Planı kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak; 657 sayılı Devlet Memurları Kanununun 125. Maddesi gereğince işlem yapılabilir ve /ve ya ilgili sözleşmelerde yer alan yaptırımlarının bir ya da birden fazla hükmü uygulanabilir. Bahsi geçen cezai işlemlerden bazıları aşağıdaki gibidir:

- Uyarma
- Kınama

- ❖ Aylıktan kesme
- ❖ Kademe ilerlemesinin durdurulması
- ❖ Para cezası
- ❖ Sözleşmenin feshi

10. PLANIN YÜRÜRLÜĞE GİRİŞİ

İşbu "**Bilgi Güveliği Planı**" Hastane Yöneticisinin onaylanmasının ardından yürürlüğe girer ve tüm personelince uyulması gereklidir.

11. PLANIN DUYURULMASI

İşbu "**Bilgi Güveliği Planı**" yürürlüğe girmesinin ardından Tüm bağlı sağlık tesislerine yazılı olarak iletilir. Kurum Web sitesine eklenir. Planının tüm personelce okunup okunmadığı ayrı ayrı her sağlık tesisinin yöneticisinin sorumluluğundadır.

12. PLAN GÖZDEN GEÇİRME KURALLARI

Bilgi Güvenliği Planı, Bilgi Güvenliği Sorumluları tarafından periyodik olarak altı ayda bir kez, üst yönetim tarafından ise yılda bir kez gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler planının gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen plan Kurum Yönetimi tarafından onaylanır. Onaylanan plan Kurum internet sitesinde yayımlanır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Bilgi Yönetimi Bölüm Kalite Sorumlusu	Kalite Yönetim Direktörü	Hastane Yöneticisi/Başhekim