1.0 AMAÇ

BGYS politikası, Menemen Devlet Hastanesi ve bağlı birimler 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.

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 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.

2.0 KAPSAM

Menemen Devlet Hastanesi ve tüm bağlı birimleri kapsar. Bilgi Güvenliği Politikası 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.

3.0 SORUMLULAR

Bu prosedürün işletilmesinden Menemen Devlet Hastanesi ve bağlı birimlerindeki tüm personeller sorumludur.

4.0 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

5.0 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.

6.0 BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

6.1 BGYS TAKIMI VE YETKİLERİ

Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü Menemen 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 işlem birimi kurulmuştur. Oluşturulan komisyon ve birimi hastane yönetimi tarafından görevlendirilme yapılarak belirlenmektedir.

6.1.1 Bilgi Güvenliği Yetkili Yöneticisi Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.
- Bilgi güvenliği yetkilisi ve/veya komisyon tarafından hazırlanmış 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 Komisyonuna başkanlık etmektir.
- Bilgi Güvenliği Biriminden, BGYS Komisyonundan gelen istek ve talepleri değerlendirmek Projelerin dayandırıldığı standartlar çerçevesinde onay vermek.
- Bilgi İşlem Biriminden, Bilgi Güvenliği YS Komisyonundan 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.

6.1.2 Bilgi Güvenliği Yetkilisi Görev ve Sorumlulukları:
- Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.
- Menemen Devlet Hastanesine bağlı birimlerde uygulanması gereken Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak ve çalışma grubuna katkı sunmak.
- Menemen Devlet Hastanesine bağlı birimlerde yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.
- Menemen 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.
- Menemen 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.

6.1.3 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.
- İzmir İl Sağlık Müdürlüğüne 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.

6.1.4 Bgys Ygg (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme)Toplantıları
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.

7.0 BİLGİ HASSASİYETİ VE RİSKLER

7.1 Bilgi Varlıklarımız Menemen Devlet Hastanesi bünyesinde tüm fiziki alanlardaki birimlerde 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.
7.2 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 Varlık Sınıflandırması

BİLGİ SINIFLANDIRMA KILAVUZU		SAKLANMA YERİ
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından 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 bilgileri T.C. Sğlık Bakanlığına bağlı tüm teşkilatına, tedarikçilerine ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

8.0 BİLGİ GÜVENLİĞİ POLİTİKASI VE KILAVUZU

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.

9.0 BİLGİ GÜVENLİĞİ GİZLİLİK SÖZLEŞMESİ, FARKINDALIK BİLDİRGESİ VE KURUMSAL GİZLİLİK TAAHHÜTNAMESİ

Kullanıcılar T.C. Sağlık Bakanlığınca hazırlanmış ve yayınlanmış Bilgi Güvenliği Farkındalık Bildirgesi ve Gizlilik Sözleşmesi imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Bilgi Güvenliği Farkındalık Bildirgesi (Kadrolu personeller), Bilgi Güvenliği Gizlilik Sözleşmesi işe alınan her firma personeli (PC kullansın kullanmasın) imzaladığı bir belgedir. Kurumsal Gizlilik Taahhütnamesi bilgi sistemlerini kapsayan tüm firmalar ile imzalanan belgedir.

10.0 BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Bilgi Güvenliği Farkındalık Eğitimleri Hizmet İçi Eğitim Kapsamına dahil edilmiş olup, her yıl düzenli olarak tüm personele eğitim verilmesi planlanmıştır.

11.0 İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

- Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
- ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
- Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) evraklar okunamaz halde geri dönüşüme gönderilmelidir.
- Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.
- Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
- Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Bilgi İşlem Birimine haber verilmelidir.

12.0 İŞE BAŞLAYIŞ, İŞTEN AYRILMA VE GÖREV DEĞİŞİKLİĞİ PROSEDÜRÜ

Menemen Devlet Hastanesi BY.PR.07 Bilgi Güvenliği İşe Başlama, İşten Ayrılma Ve Görev Değişikliği Süreç Prosedürüne uygun olarak hareket edilmelidir.

13.0 BİLGİ KAYNAKLARI VE ATIK İMHA YÖNETİMİ POLİTİKASI

Menemen Devlet Hastanesi BY.PR.08 Basılı Ortam ve Bilgilerin Anonim Hale Getirilmesi ve İmha Edilmesi Prosedürü ile BY.PR.04 Bilgi Saklama Ortamları Yok Etme Prosedürüne uygun olarak hareket edilmelidir.

14.0 İHLAL BİLDİRİM VE YÖNETİMİ

- 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 durumlarında mutlaka kayıt altına alınmalıdır.
- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
- İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
- Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.
- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.
- Bilgi Güvenliği İhlali Tespit edilmesi Durumunda BY.YR.08 Olay Bildirimi Müdahale Formu doldurulmalıdır.
- Merkezi İhlal Bildirim Sisteminin Kullanılacağına Yönelik Eğitim verilmesi planlanmıştır.

15.0 İNTERNET VE ELEKTRONİK POSTA GÜVENLİĞİ

Menemen Devlet Hastanesi kullanıcılarına BY.PR.05 İnternet ve E-posta Kullanım Prosedürüne uygun olarak hareket edilmelidir.

16.0 MAL VE HİZMET ALIMLARI GÜVENLİĞİ

Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

17.0 SOSYAL MÜHENDİSLİK ZAAFİYETLERİ VE SOSYAL MEDYA GÜVENLİĞİ POLİTİKASI

Menemen Devlet Hastanesi BY.PR.06 Sosyal Mühendislik Zaafiyetleri Ve Sosyal Medya Güvenliği Prosedürüne uygun olarak hareket edilmelidir.

18.0 POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği Politikası 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

19.0 POLİTİKANIN YÜRÜRLÜĞE GİRİŞİ

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

20.0 POLİTİKANIN DUYURULMASI

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

21.0 POLİTİKANIN GÖZDEN GEÇİRME KURALLARI

Bilgi Güvenliği Politikası, 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 Politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen Politika Kurum Yönetimi tarafından onaylanır. Onaylanan Politika Kurum internet sitesinde yayımlanır.

22.0 EKLER

- BY.PR.07 Bilgi Güvenliği İşe Başlama, İşten Ayrılma Ve Görev Değişikliği Süreç Prosedürü
- BY.PR.08 Basılı Ortam ve Bilgilerin Anonim Hale Getirilmesi ve İmha Edilmesi Prosedürü
- BY.PR.04 Bilgi Saklama Ortamları Yok Etme Prosedürü
- BY.YR.08 Olay Bildirimi Müdahale Formu
- BY.PR.05 İnternet ve E-posta Kullanım Prosedürü
- BY.PR.06 Sosyal Mühendislik Zaafiyetleri Ve Sosyal Medya Güvenliği Prosedürü