**1. AMAÇ**
Ermenek Devlet Hastanesi Bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir.

**2.KAPSAM**
Ermenek Devlet Hastanesi Bilgi Güvenliği Politika metninde yer alan kapsam maddesinde
belirlenmiş olan kapsamdır.

**3.POLİTİKA METNİ**

3.1 Kişisel verilere erişim verilen yetki dahilindedir.

3.2 Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.

3.3 Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.

3.4 Çok gizli evraklar çelik kasalarda saklanmakta olup sadece yetki verilen personel ulaşmaktadır.

3.5 Personel görev yaptığı birimle ilgili bilgiye ulaşabilmekte diğer bilgilere ulaşamamaktadır.

3.6 Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

3.7 Erişim izinleri verilirken, “görevlerin ayrılığı” ve “bilmesi gereken” prensiplerine göre hareket edilir.

3.7.1 “Görevlerin ayrılığı” prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için bi.rden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

3.7.2“Bilmesi gereken” prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

3.7.3 Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılabilir.

3.7.4 Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu, varlık sahipleri tarafından belirlenir.

3.7.5 Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

3.7.6 Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

3.7.7 Bilgi varlıklarına fiziksel olarak yapılacak erişimler için bu yönergenin [A.8](#_bookmark22) maddesinde belirtilen önlemler alınır.

**3.7.8 Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu’nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.**

**3.8 Bilgi Yönetim Sistemine ilişkin rol grupları ve yetkileri:** Otomasyon üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılmıştır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir.

3.8.1 Bu rol grupları; • Üst Yönetim(Başhekim, Başhekim Yardımcısı,Müdür ve Müdür Yardımcısı) • Hekim • Ebe,Hemşire ve Sağlık Personeli • Eczacı • Poliklinik Sekreteri • Maaş Mutemet • Kalite • Faturalama vb. Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır.Aynı görevde çalışan personellerin yetkileri de aynıdır.İşe yeni başlayan personel bilgi işlemden kullanıcı yetkilendirme ile kullanıcı adı ve şifresi verilir.İşten ayrılırken ise ilişik kesmek için bilgi işleme başvurarak ilişik kesilir. Her kullanıcının BYS uygulamalarında hangi bilgilere erişebileceği tanımlanmıştır. Çalışanlar yetki düzeyleri ile ilgili olarak bilgilendirilir. Bilgilendirme ve yetki düzeyi kayıt altına alınmıştır.Aynı görevde çalışanlar aynı yetki gruplarına sahip olacak şekilde yapılmıştır.

**3.9 Disiplinler arası yetkilendirme aşağıdaki gibidir:**

**3.9.1 Başhekim:** Hastanedeki tüm bilgilere ulaşır.

**3.9.2 Müdür:** İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

**3.9.3 Doktor:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken tüm hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir. Hasta ‘Adli Olgu’ ise hasta raporu ancak Uzman tarafından girilebilir ve aynı Uzman tarafından onaylandıktan sonra değiştirilemez.

**3.9.4 Ebe-Hemşire ve Sağlık Memuru:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait işleri yetkileri dahilinde yapabilirler.

**3.9.5 Personel Sicil Birimi:** Personel özlük bilgilerine ulaşabilir, mesai, izin, sevk, rotasyon gibi personelin tüm işleyişini otomasyon üzerinden gerçekleştirir.

**3.9.6 Maaş Mutemet:** Personele yapılacak ödemeleri otomasyon sistemi üzerinden yapar.

**3.9.7 Tig Birimi Personeli:** Yetkisi dahilinde tig işlemlerini yapar.

**3.9.8 Faturalama Birimi Personeli**: Hastaya ait faturalama işlemlerini yetkisi dahilinde yapar.

**3.9.9 Eczane:** Katlardan gelen eczaneyle ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar.

**3.9.10 Radyoloji:** Hastaların radyolojik işlemlerini yapar.

**3.9.11 Laboratuvar:** Doktorların hastaları için, yaptığı istemleri alır, çalışmasını yapar ve otomasyon üzerinde laboratuvar işlemlerini yapar.

**3.9.12 Poliklinik Sekreteri:** Hastaların gelişte otomasyon programına kayıtlarını yapar. Her kademedeki çalışan sadece yetkilendirilmiş olduğu işlemleri yürütebilmektedir.

**3.9.13 Bilgi İşlem Personeli:** Bilgi işlem birimi personelleri hastane otomasyon sisteminde sorunlara müdahale, yetkilendirme işlemleri ve üst yönetime istatistiki rapor için tüm yetkilere sahip olup, gizlilik kuralları çerçevesinde işlemlerini yapmaktadır.

 3.10 Tüm çalışanlar otomasyon üzerinde yetkili oldukları bilgileri herhangi bir şekilde farklı ortamlarda paylaşamaz bilgi taşıyamaz. Kullanılan yazılımlarla ilgili şifreler kullanıcılara Bilgi İşlem tarafından verilir ve belli periyotlarda değiştirilmesi istenir. Yetkilendirilen çalışan, şifrelerin kullanılması ve korunması konusunda sorumlu tutulmaktadır.

# 4.YAPTIRIM Bu politikanın ihlali durumunda, BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.