1. AMAÇ: Bu prosedürün amacı Adana Seyhan Devlet Hastanesinde bilgiye erişimi kontrol etmek için yöntemlerin oluşturulmasıdır.

2. KAPSAM: Bu prosedür Adana Seyhan Devlet Hastanesinde bilgiye erişimin kontrolü ile ilgili kuralları kapsar.

3. KISALTMALAR:

SBYS: Sağlık Bilgi Yönetim Sistemi.

4. TANIMLAR:

5. SORUMLULAR: SBYS hizmet alım firması ve hastane idaresi

6. FAALİYET AKIŞI:

Erişim kontrol politikası hazırlanırken aşağıda sıralanan prensipler dikkate alınır:

6.1. 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.

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

6.3. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

6.4. Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

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

6.6. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir. Yetkilendirme bilgi işlem firması ve idare tarafından ortaklaşa mutabakat ile belirlenerek, yetkilendirilmiş kişilerin hangi verilere ulaşacağı SBYS yazılımı "yetkilendirme tablosu " üzerine belirtilir ve görülebilir.

6.7. Yetkilendirme tablosunda rol bazlı yetkilendirme yapılmıştır. Yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi engellenmiştir.

6.8. Rol bazlı yetkilendirme acil laboratuvar, acil servis sekreter, arşiv, ameliyathane sekreteri, hemşire/ebe, diyetisyen, doktorlar, ds komisyon, eczane, faturalama, istatistik, kan bankası, kalite, laboratuvar, odyometri, radyoloji teknisyen, sağlık kurulu, servis sekreterliği, sorumlu hemşire, supervisor, tıbbi pataloji, uzman biyokimya, vezne, yönetici, poliklinik sekreter, enfeksiyon hemşiresi, tıbbi atık, insan kaynakları, satınalma, tıbbi sarf, depolar, mutemetlik, radyoloji hekimleri, uzman pataloji, uzman mikrobiyoloji, psikometri, danışma gibi grupları ifade etmektedir.

6.9. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden 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.

6.10. **"**Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

6.11. 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.
6.12. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu varlık sahipleri tarafından belirlenir.
6.13 Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. VTYS sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

7. KULLANICI ERİŞİMLERİNİN YÖNETİMİ

7.1. Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.
7.2. Başta kişisel sağlık verilerinin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne tabi tutulacak tüm sistem ve hizmetler için "kullanıcı erişim yönetimi esasları" belirlenir. Belirlenen esaslar, ilgili tüm taraflara (muhtemel kullanıcılara) resmen duyurulur.
7.3. Kullanıcı erişimleri ile ilgili yönetim esasları belirlenirken aşağıdaki hususlar dikkate alınır:

- Hizmet veya sisteme erişim için nasıl müracaat edileceği,
- Müracaat esnasında hangi bilgilerin isteneceği,
- Kullanıcıların yetkilendirilmesinde kullanılan roller ve haklarının neler olduğu,
- Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağı,
- Ayrıcalıklı erişim taleplerinin nasıl değerlendirileceği,
- Kullanıcı erişimlerinin izlenmesi için alınmış olan tedbirler,
- Kullanıcı hesaplarının kapatılması/silinmesi için yapılacak işlemler.

7.4. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.
7.5. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 (altı) aylık aralıklarla yapılır.
7.6. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.
7.7. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, 3 (üç) ayı aşmayacak şekilde daha sık yapılır.
7.8. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre bilgi güvenliği alt komisyonu tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.
7.9. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur. Mümkün olduğu yerlerde, rutin ve düzenli sistem yönetim işlevlerinin otomatik araçlarla (batch/otomatik kod yazılması, sistem yeteneklerinin kullanılması vb.) yapılması sağlanır.
7.10. Ayrıcalıklı erişim hakları, düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliğine tahsis edilir. Düzenli iş faaliyetleri, ayrıcalıklı kullanıcı kimliği ile yapılmaz.
7.11. Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanır ve sıkı bir şekilde kontrol edilir.

7.12. Programların kaynak kodları ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçerleme planları gibi) erişim (yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için) sıkı bir şekilde kontrol edilir.

8. AYRICALIKLI ERİŞİM HAKLARININ YÖNETİMİ

Ayrıcalıklı erişim hakları; veritabanı, PACS, Web, uygulama sunucuları ile hastane genelindeki bilgisayarlar üzerinde yalnızca HBSY destek personelinin ve Bilgisayar Destek Birimi kadrolu personelinin domain sistemindeki kullanıcılarına verilmektedir. Diğer personelin ayrıcalıklı erişim hakları kısıtlanmıştır. '**Ayrıcalıklı Erişim Hakkı Talep Formu"** ile ayrıcalıklı erişim yetkisi verilir.

9. KULLANICILARA AİT GİZLİ KİMLİK DOĞRULAMA BİLGİLERİNİN YÖNETİMİ

Gizli kimlik bilgisi olarak parolalar kullanılmaktadır. Kullanıcı oturumun ilk sağlanmasında kullanıcıya ilk kullanımda parola değişiklik yapılması için uyarı verir.

10. ERİŞİM HAKLARININ KALDIRILMASI VEYA DÜZENLENMESİ

Erişim hakları personelin ayrılışı durumunda İşten Ayrılma Formu ile üzerinde bulunan kullanıcıya ait erişim hakları kaldırılır. Erişim haklarının gözden geçirilmesi sonucunda herhangi bir düzenleme yapılması durumunda '**Bilgi Sistemleri Erişim ve Yetkilendirme Talep Formu"** düzenlenir.

11. İLGİLİ DÖKÜMANLAR

Yetkilendirme Tablosu