ERİŞİM KONTROL POLİTİKASI

1.AMAÇ: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumları kapsamındaki 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: Bu politika, Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumları bünyesindeki bilgi ve bilgi işleme tesislerine erişim sağlayan tüm kullanıcılar içindir.

3.POLİTİKA METNİ

3.1.BELGE YÖNETİM SİSTEMİ VE DİJİTAL ARŞİV ERİŞİMİ

3.1.1. Kurum Elektronik Belge Yönetim Sistemi (EBYS) kullanıcı tanımlamaları Müdür Oluru ile görevlendirilen EBYS İl Yetkililerince gerçekleştirilir.

3.1.2. EBYS'de personel tanımlamaları kullanıcının tanımlanacağı birim yöneticisi onayı ile yapılır. Birim evrak görme gibi özel yetkilendirmeler özellikle bildirilir. Personelin birim / görev değişikliği olması halinde birim yöneticisi tarafından İl yetkilisine kullanıcının pasife alınması / yetki iptali için bilgi verilir.

3.1.3. Sağlık Bakanlığı EBYS kullanılmaya başlandığında bağlı kurumların dijital arşivleri EBYS sisteminde bulundurulduğundan farklı bir arşiv sistemi kullanılmamaktadır. Tanımlı her kullanıcı kendi birim arşivine sistem üzerinden ulaşabilmektedir. Kurum arşivine yalnız kurum evrak kayıt yetkisi tanımlı kullanıcılar erişebilir.

3.1.4.2017/21 Sayılı Başbakanlık Genelgesi gereği "çok gizli, gizli, özel ve hizmete özel" yazılar elektronik ortamda gönderilmemektedir. Bu gizlilik dereceli sınıflandırmaya giren yazışmalarda evraklar, kapalı ve mühürlü zarf içinde elden ve ya güvenli posta yoluyla taşınmalıdır. Genelgeye göre "çok gizli" evraklar bakanlık ve genel müdürlükçe tayin edilmiş kişiler tarafından verilir ve mahfuz odalar, kilitli çelik dolaplar, kasa, çelik masa içerisinde muhafaza edilmelidir. "Gizli, özel ve hizmete özel evrak dereceleri ise yazıyı hazırlayan memur tarafından tayin edilir. "Gizli ve özel" evraklar kilitli çelik dolaplarda, "hizmete özel" evraklar ise kilitli kalmak koşulu ile masa gözlerinde saklanmalıdır.

3.2.SAĞLIK BİLGİ YÖNETİM SİSTEMLERİ ERİŞİMİ

3.2.1. Sağlık Bilgi Yönetim Sistemleri, Sağlık Tesisleri idari, tıbbi ve mali tüm hizmet birimlerince kullanılan otomasyon ve görüntüleme sistemlerini kapsar.

3.2.2. Sağlık Bilgi Yönetim Sistemleri (SBYS) barındırdığı kurumsal bilgi ve kişisel veri dolayısıyla bilgi güvenliği açısından büyük önem arz eder.

3.2.3. Her Sağlık Tesisinde SBYS Yetkilisi/ Yetkilileri, Başhekim Oluru ile belirlenir. SBYS Yetkilisi Personel Gizlilik Sözleşmesi imzalar.

3.2.4.SBYS Yetkilisi yazılım modüllerini kullanarak erişim rolleri oluşturur. Rollere göre kullanıcı yetkilendirilir. Kullanıcı yetkilendirmeleri, kullanıcı görev ve sorumlulukları doğrultusunda bağlı yönetici onayı ile yapılır.

3.2.5. Kullanıcıların SBYS erişim ve gezintileri kayıt altına alınır.

3.2.6. Kullanıcıların görev değişikliği işten ayrılma gibi durumlarda yetkisiz erişimleri önlemek adına yetkileri kaldırmak için SBYS Yetkilisine bildirim yapmak, kullanıcının bağlı olduğu ilk yönetici sorumluluğundadır.

3.2.7.SBYS Kullanıcı tanımlama ve parola belirleme işlemlerinde Müdürlüğümüz Parola Politikası uygulanır. Yetkilendirilmiş kullanıcı, kendi parolası ile oturum açarak sistem üzerinde yaptığı tüm işlemlerden sorumludur.

3.2.8. Kullanıcı sistem üzerinde yaptığı işlemlerde 6698 sayılı Kişisel Verileri Koruma Kanunu'na uymakla yükümlüdür.

3.2.9. Kullanıcı iş bitiminde oturum kapatmakla yükümlüdür. Açık unutulmuş veya başkası ile şifre paylaşılarak açılmış oturumlarda yapılan ihlallerden parolası ile oturum açılmış olan kullanıcı sorumludur. Hakkında Müdürlüğümüz Disiplin Prosedürü ilgili maddeleri işleme konulacaktır.

3.3. VERİ TABANI YÖNETİM SİSTEMLERİNE ERİŞİM

3.3.1. Veri tabanında kullanıcı hesabı oluşturma ve kullanıcılara erişim yetkisi tanımlama talepleri resmi yazı ile yapılır.

3.3.2.Müdürlük ve bağlı tüm kurumlarında bulunan veri tabanına erişen kullanıcılar (veri tabanı yöneticileri, uygulama geliştiriciler, yedekleme operatörleri vb.) ile mutlaka gizlilik sözleşmesi imzalanır ve erişim hakkı edindikten sonra almış olduğu sorumluluklar kullanıcıya bildirilir.

3.3.3. Veri tabanında sorgu seviyesindeki erişim denetimleri 3 ayda bir kontrol edilir. Erişim denetiminin tablo seviyesinde mi yoksa satır/sütun seviyesinde mi olduğu kullanıcının rolüne göre belirlenir ve kurum erişim kontrol politikasında belirtilen kurallar dâhilinde yetki tanımlaması yapılır.

3.3.4. Veri tabanına erişim sağlayan kullanıcılar için kimlerin nereye erişim sağlayacağı gibi erişimler sınıflandırılır. Zaman içerisinde değişen kullanıcı erişim yetkileri, audit (izleme/denetim) kurallarıyla takip edilir.

3.3.5. Veri tabanına erişen ortak kullanıcı hesaplarına izin verilmemelidir.

3.3.6. Uygulama sunucuları üzerinden gelen veri tabanı kullanıcılarının, sadece ilgili uygulama sunucularından bağlantı sağlaması, okuma, yazma, silme ve değiştirme yetkileri olması; yeni tablo/nesne oluşturma, şema değişikliği yapma gibi yetkilerinin kaldırılması gerekir.

3.3.7. Benzer şekilde veri tabanı sunucularına kod geliştiren kullanıcı için oluşturulan veri tabanı kullanıcılarının da yeni tablo/nesne oluşturma, şema değişikliği yapma gibi yetkilerinin olması bunun dışında canlı/gerçek veriye erişerek bu veriler üzerinde okuma, yazma, silme ve değiştirme gibi yetkilerinin olmaması gerekir.

3.3.8. Veri tabanında yer alan tüm kullanıcı hesaplarının durumları düzenli olarak kontrol edilir. Veri tabanında oluşturulmuş isimsiz hesaplar, geçmişte açılmış fakat kullanılmayan hesaplar özellikle kontrol edilmeli, kurumdan ayrılan çalışanlara ait veri tabanı hesapları kilitlenir veya silinir.

3.3.9."Yedek alabilme" hakkına sahip kullanıcı hesapları, aynı şekilde düzenli olarak kontrol edilir.

3.3.10. Veri tabanları arasında veri aktarımı yapmak için kullanılan database linkleri "private" olarak oluşturulur. Güvenlik açığı teşkil etmesi nedeniyle "public" olarak oluşturulmuş linkler, "private" olarak değiştirilmelidir. Tüm linkler belirli aralıklarla kontrol edilir.

3.3.11. Veri tabanına yapılan erişimlerde kaba kuvvet saldırılarına karşı, kullanıcı hesabının kitlenmesi için giriş kontrolü yapılmalıdır (5 (beş) yanlış deneme sonrası kullanıcı hesabının kilitlenmesi gibi).

3.3.12. Veri tabanına bağlanan kullanıcıların, görüntülediği verileri aktarma veya tablo dışına çıkarma gibi yetkileri/işlemleri için kontrol mekanizmaları sağlanır. Verilerin elektronik kopyasının alınması gerekli ise verilen yetkiler gözden geçirilir.

3.3.13. Veri tabanına son girilen başarılı ve başarısız oturum bilgilerinin giriş kayıtları tutulur.

3.3.14. Veri tabanında kritik rollere sahip kullanıcıların yetkileri ve görevleri, kurum erişim kontrol politikasında belirtilen aralıklarla düzenli olarak kontrol edilir. Varsa gereğinden fazla verilmiş olan yetkiler kaldırılır.

3.3.15. "Select" yetkisi dışında yetkisi olan kullanıcılar ayrıştırılarak bu kullanıcılar birer aylık aralıklarla kontrol edilir. Veri tabanı sunucuları için kod geliştiren kullanıcılar dışında diğer kullanıcıların veri tabanına bağlanıp sorgu yapmaları engellenir(örnek; Kullanıcıların tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmaları engellenir) .

3.3.16. Veri tabanında "sysdba, sysoper, admin" yetkisine sahip olan kullanıcı hesaplarının kontrolleri yapılır. En yetkili kullanıcıların veri tabanında yaptığı işlemler kayıt altına alınır.

3.3.17. SQL Server kurulumu ile gelen varsayılan "SA" kullanıcısı pasife alınır.

3.3.18. Veri tabanında sahip olduğu yetkileri bir başka kullanıcıya ("withadminoption" ya da "withgrantoption" gibi seçeneklerle) devretme yetkisi olan kullanıcı hesapları özellikle takip edilir. Mutlak zorunluluk yok ise kullanıcılara bu tür yetkiler verilmemelidir.

3.3.19. Veri tabanı yönetim sistemlerinin, alanında uzman ve eğitim almış personel tarafından yönetilmesi sağlanır.

3.3.20. Güvenlik paketleri ve yamalar, kontrollü olarak uygulanır. Sistemde hangi yamaların uygulanıp uygulanmadığı kontrol edilir.

3.3.21. Veri tabanı sunucusu sadece SSH, RDP, SSL ve veri tabanının orijinal yönetim yazılımına açık tutulur. Bunun dışında FTP, TELNET vb. gibi açık metin şifreli bağlantılara kapatılır.

3.3.22. Veri tabanı sistemlerinde tutulan bilgiler kurumun yedekleme politikasına uygun olarak yedeklenir. Resmi yazı ile belirlenmiş, yedeklemeden sorumlu sistem yöneticileri tarafından yedeklerin tutanak altında düzenli olarak alınması takip edilir.

3.3.23. Veri tabanından alınan yedeklerin başarılı olarak alındığı iz kayıtları üzerinden kontrol edilir. Kurumun bilgi güvenliği alt komisyonu tarafından belirlenecek yedekleme politikaları uyarınca geri dönüş testleri yapılır.

3.3.24. *Veri tabanı kullanıcı profillerine göre tanımlanması gereken parola parametreleri ve önerilen değerleri şu şekildedir*:

3.3.24.1. Kullanıcı hesabının kilitlenmesi için gerekli maksimum başarısız oturum açma girişim sayısı 5 (beş),

3.3.24.2. Parolanın geçerli sayılacağı maksimum gün sayısı 90 gün,

3.3.24.3. Kullanıcı parola süresi dolmadan önce kullanıcıya parolasını değiştirmesi için hatırlatma gönderme süresi 7 (yedi) gün,

3.3.24.4. Parolanın tekrar kullanılabilmesi için tanımlanması gereken minimum farklı parola sayısı 3 (üç),

3.3.24.5. Maksimum sayıdaki başarısız oturum açma girişimlerinden sonra, hesabın ne kadar süreyle kilitli kalacağı süre 10 (on) dakika.

3.3.24.6. Veri tabanı kullanıcıları ilk kez tanımlanan hesaplarıyla oturum açtıklarında parola değiştirmeye zorlanır.

3.3.25. Veri tabanı sunucusu üzerindeki gereksiz olan servisler kapatılır.

3.3.26. Sistem üzerinde bilgi toplanmasına neden olabilecek başlık bilgileri ve hata mesajlarının açık bırakılması önlenir.

3.4. KİŞİSEL VERİLERE ERİŞİM

3.4.1. Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi kapsar.

3.4.2. Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem tanımlanır.

3.4.3. Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi,

b)Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

c)Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,

f)İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

3.4.4. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. Sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. Özel nitelikli kişisel verilerin işlenmesinde, ayrıca "Kişisel Verileri Koruma Kurulu "tarafından belirlenen yeterli önlemlerin alınması şarttır.

3.4.5. Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

3.4.6. Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

Yeterli korumanın bulunduğu ülkeler Kişisel Verileri Koruma Kurulunca belirlenerek ilan edilir.

Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve aktarıma izin verilip verilmeyeceğine;

a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,

b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,

c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,

ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,

d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir. Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

3.4.7. Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

3.4.8."25.01.2018 tarihli ve 30312 sayılı Resmî Gazete'de yayımlan, Kişisel Verileri Koruma Kurulu tarafından alınan 21.12.2017 tarihli ve 2017/62 sayılı Kurul Kararı" gereği: "6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesi" uyarınca banko, masa ve gişe gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek, aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirlerin alınması gerekmektedir.

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.