1. AMAÇ

Yalova İl Sağlık Müdürlüğü ve bağlı tesislerin bünyesinde bilgiye erişimi kontrol etmek için yöntemlerin oluşturulmasıdır.

2. KAPSAM

Erişim kontrolü bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, yetkisiz kullanıcı erişimine izin verilmemesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanması gibi kritik konuları kapsamaktadır. Bu denli kritik bir konuda güvenliğin sağlanması için aşağıdaki maddeler göz önünde bulundurulmalıdır;

3. POLİTİKA

3.1-Erişim Kontrolü İçin İş Gereksinimleri

3.1.1-Erişim Kontrolü Politikası

- ✓ Erişimle ilgili iş ve güvenlik ihtiyaçları göz önünde bulundurularak erişim kontrol politikası oluşturulmuş ve belgelenmiş olmalıdır.
- ✓ Erişim kontrol hem fiziksel hem de işlevsel boyutları ile değerlendirilmiş olmalıdır.
- ✓ Erişim kontrolü politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını açıkça belirtiyor olmalıdır.
- ✓ Kullanıcılara ve servis sağlayıcılarına erişim kontrolüyle hangi iş gereksinimlerinin karşılanacağı iyice açıklanmış olmalıdır.
- ✓ Politika belgesi şu konuları içermelidir; her bir iş sürecinin güvenlik ihtiyaçları, iş süreçleri ile ilgili tüm bilgiler ve bu bilgilerin yüz yüze olduğu riskler, bilginin yayılması ve yetkilendirme ile ilgili politikalar, bilginin sınıflandırılması, güvenlik seviyeleri ve "gerektiği kadar bilme" prensibi, farklı sistem ve ağlardaki bilginin sınıflandırılması ve erişim kontrolüne ilişkin politikaların tutarlı olması, bilgiye erişimle ilgili olarak kontratlardan ve yasal yükümlülüklerden kaynaklanan şartların yerine getirilmesi, kurumun yaygın kullanıcı profilleri ile ilgili erişim hakları ve Erişimin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması.
- ✓ Erişim haklarının "Yasaklanmadıkça her şey serbesttir" değil "İzin verilmedikçe her şey yasaktır" prensibine göre verilmesine dikkat edilmelidir.

3.2-Kullanıcı Erişiminin Yönetilmesi

3.2.1-Kullanıcı Kaydı:

- ✓ Bilgi sistemlerine ve servislerine erişim hakkı vermek için resmi bir kullanıcı kaydı girme ve kullanıcı kaydı silme prosedürü olmalıdır.
- ✓ Sistem kayıtları ile ilişkilendirme ve sorumlu tutulabilme açısından kullanıcı kimliklerinin her kullanıcı için farklı olmasına dikkat ediliyor olmalıdır.
- ✓ Bilgi sistemini ve servisini kullanabileceğine dair sistem sahibi kullanıcıya yetki vermiş olmalıdır.
- ✓ Verilen erişim hakkı kurumsal güvenlik politikasına ve görevler ayrılığı ilkesine uygun olmalıdır.
- ✓ Kullanıcılara erişim hakları ile ilgili yazılı belge veriliyor ve kullanıcılardan erişim şartlarını anladıklarına ilişkin imzalı belge alınıyor olmalıdır.
- ✓ Görevi değişen veya kuruluştan ayrılan personelin erişim hakları derhal güncellenmelidir.

3.2.2-Ayrıcalık Yönetimi:

- ✓ Ayrıcalıkların kullanımı sınırlandırılmış ve denetleniyor olmalıdır.
- ✓ Ayrıcalıklar "kullanması gereken" prensibine göre ve resmi bir yetkilendirme süreci sonunda verilmelidir.

3.2.3-Kullanıcı Parola Yönetimi

- ✓ Kullanıcı parolalarının atanması ya da değiştirilmesi resmi bir prosedür uyarınca yapılmalıdır.
- ✓ Kullanıcılara parolalarını saklı tutacaklarına dair bir anlaşma imzalatılmalıdır.

3.2.4-Kullanıcı Erişim Haklarının Gözden Geçirilmesi

- ✓ Kullanıcı erişim haklarının düzenli aralıklarla kontrol edilmesini sağlayan resmi bir süreç olmalıdır.

3.2.5-Parola Kullanımı

- ✓ Kullanıcı parolalarının seçilmesi ve kullanılması ile ilgili güvenlik tedbirleri uygulanmalıdır.
- ✓ Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi sağlanmalıdır.
- ✓ Kullanıcılar zor kırılacak parolalar seçmeleri konusunda bilinçlendirilmiş olmalıdır.
- ✓ Kişisel parolaların hiç kimse ile paylaşılmamasına, yazılı veya elektronik ortamlarda kaydedilmemesine dikkat edilmelidir.
- ✓ Kullanıcılar düzenli aralıklarla veya sistem güvenliği ile ilgili bir kuşku oluştuktan sonra parolalarını değiştirmeye zorlanmalıdır.
- ✓ Kullanıcılar kişisel işlerinde kullandıkları parolaları kuruluşun iş süreçlerinde kullanmamaları gerektiği konusunda bilinçlendirilmiş olmalılardır.

3.2.6-Gözetimsiz Kullanıcı Ekipmanı

- ✓ Âtıl cihazlara ait güvenlik gereksinimlerinden, bu cihazları koruma prosedürlerinden ve bu cihazları korumak için üzerlerine düşen sorumluluklardan kullanıcıların ve iş ortaklarının haberleri olmalıdır. (İşi biten kullanıcıların bilgisayarını kapatması ve şifreli ekran koruyucuların kullanılması gibi)

3.3-Ağ Erişim Kontrolü

3.3.1-Ağ Hizmetlerinin Kullanılması İle İlgili Politikalar

- ✓ Kullanıcıların sadece kullanma yetkisine sahip oldukları ağ servislerine erişebilmesi sağlanmış olmalıdır.
- ✓ Ağlar ve ağ servisleri ile ilgili olarak şu konuları düzenleyen politikalar uygulanıyor olmalıdır; kimin hangi ağlara ve ağ servislerine erişebileceğini belirlemek için yetkilendirme prosedürü tanımlanmış olmalıdır, ağ bağlantılarını korumak ve ağ servislerine erişimi engellemek için yönetim denetimleri ve süreçleri belirlenmiş olmalıdır.

3.4-Harici Bağlantılar İçin Kullanıcı Kimliği Doğrulaması

- ✓ Sisteme dışarıdan yapılacak kullanıcı bağlantıları için kullanıcı kimliği doğrulama mekanizmaları uygulanmalıdır. (Kripto tabanlı teknikler veya klasik "challange-response" mekanizmaları ile çözülebilir. VPN çözümleri de bu teknikleri kullanmaktadır.)

3.5-Ağlarda Cihaz Kimliği Belirleme

- ✓ Bağlantının belli bir cihaz kullanılarak yapıldığından emin olmak için otomatik cihaz kimliği belirleme yöntemleri kullanılıyor olmalıdır.

3.6-Uzaktan Tanı ve Yapılandırma Portu Koruma

- ✓ Yönetim ve yapılandırma portlarına fiziksel ve işlevsel erişimi denetleyen bir güvenlik mekanizması olmalıdır.

3.7-Ağlardaki Ayrım

- ✓ Bilgi sistemi üstündeki kullanıcı ve servisler gruplara ayrılmış olmalıdır.
- ✓ Kurumun ağı dahili ve harici etki alanlarına bölünmüş olmalıdır.
- ✓ Etki alanları kurumun erişim kontrol politikası ve erişim ihtiyaçları uyarınca oluşturulmuş olmalıdır.
- ✓ Etki alanları sınır güvenliği sistemleri ile korunmalıdır.
- ✓ Telsiz ağların diğer ağlardan ayrılması ile ilgili olarak çalışma yapılmış olmalıdır.

3.8-Ağ Bağlantı Kontrolü

- ✓ Kurum sınırlarının dışına taşan ağlar ve ağ bağlantılarının kullanımı, kurumun erişim kontrol politikası uyarınca kısıtlanmış olmalıdır.
- ✓ Elektronik mesaj, tek veya çift yönlü dosya aktarımı, interaktif erişim, bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilmiş olmalıdır.

3.9-Ağ Yönlendirme Kontrolü

- ✓ Ağ yönlendirme kontrolleri, bilgisayar bağlantılarının ve bilgi akışının erişim politikasına uygun gerçekleşmesini sağlayacak şekilde tanımlanmış olmalıdır.
- ✓ Ağ iletişimi kaynak adres ve hedef adreslere bağlı olarak güvenlik duvarı vb. cihazlar aracılığı ile kontrol ediliyor olmalıdır.

3.10-Güvenli Oturum Açma Prosedürleri

- ✓ Oturum açma işlemleri yetkisiz erişim olasılığını asgari düzeye indirecek şekilde düzenlenmiş olmalıdır.
- ✓ Sistem ve uygulamaya ilişkin olarak yetkisiz kullanıcıya yardımcı olabilecek bilgiler oturuma giriş başarıyla tamamlanana kadar gizlenmelidir.
- ✓ Bilgisayarda sadece yetkili personel tarafından erişilebileceğini bildiren uyarı mesajı gösterilmelidir.
- ✓ Oturuma giriş sadece tüm girdi verilerinin doğrulanmasından sonra sağlanmalıdır.

- ✓ Bir hata durumu varsa sistem verinin hangi kısmının doğru veya yanlış olduğu bilgisini gizlemelidir.
- ✓ Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmiş olmalıdır.
- ✓ Oturuma giriş işlemi için zaman sınırı olmalıdır.
- ✓ Başarısız giriş denemeleri kaydedilmelidir.
- ✓ Ağ üstünden şifrenin açık olarak gönderilmemesi sağlanmalıdır.