SAMSUN İL SAĞLIK MÜDÜRLÜĞÜ ERİŞİM KONTROL VE UZAKTAN ERİŞİMİ POLİTİKASI

T.C. SAĞLIK BAKANLIĞI
SAMSUN
İL SAĞLIK MÜDÜRLÜĞÜ

AMAÇ

Bu dokümanın amacı 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 edilmesini amaçlamaktadır.

1. ERİŞİM KONTROL POLİTİKASI

1.1. Tüm sağlık tesislerimizde 'erişim yetki ve kontrol matrisi' oluşturulacaktır. Erişim yetki ve kontrol matrisinde kimin hangi bilgiye, hangi yetkilerle erişeceği ve erişimin kontrolü için yapılacak yöntemler yer alacaktır.

1.2. Erişim yetki ve kontrol mekanizması oluşturulurken aşağıda belirtilen prensipler dikkate alınır:

1.2.1. 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.

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

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

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

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

1.2.6. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

1.2.7. "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.

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

1.2.9. 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.

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

1.2.11. Sağlık Bilişim Ağı (SBA) 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.

1.2.12. 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. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için Fiziksel ve Çevresel Güvenlik politikasında belirtilen önlemler alınır.

1.2.13. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK'nın 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.

Hazırlayan	Kontrol Eden	Onaylayan
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü

1.3. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.
1.4. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 aylık aralıklarla yapılır. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili 3 ayı aşmayacak şekilde daha sık yapılır.
1.5. 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.
1.6. Ayrıcalıklı erişim hakları, düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliğine tahsis edilir. Düzenli iş faaliyetleri, ayrıcalıklı kullanıcı kimliği ile yapılmaz.
1.7. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.
1.8. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri idarede yetkili personellere teslim edilmelidir.
1.9. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.
1.10. Kurumun yedekleme sistemlerine sadece memur ya da birim sorumlusu yetkili kişi erişim yapmalıdır Firmaların yapacakları tüm işlemler birim sorumlusu nezaretinde yürütülmelidir.
1.11. Kurumun güvenlik cihazlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır.
1.12. Kurumun veri tabanlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır
1.13. Kurumun network cihazlarına ait loglar kurum tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde işbirliği içinde raporlar paylaşılmalıdır
1.14. Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.
1.15. Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.
1.16. Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.
1.17. Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.
1.18. Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.
1.19. Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

Hazırlayan	Kontrol Eden	Onaylayan
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü

2. UZAKTAN ERİŞİM YÖNETİMİ (AYRICALIKLI ERİŞİM)

2.1. Uzak erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptirler.
2.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanılacaktır.Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir. Detaylı bilgilendirme Bilgi Güvenliği Politikaları Kılavuzunda mevcuttur.
2.3. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
2.4. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir.
2.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
2.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
2.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
2.8. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
2.9. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır
2.10. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
2.11. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.
2.12. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.
2.13. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.
2.14. 6698 sayılı Kanun'un açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.
2.15. Dokümanda yer almayan maddeler için Bakanlığımız Bilgi Güvenliği Politikaları Kılavuzunda yer alan hususlar geçerlidir.

Hazırlayan	Kontrol Eden	Onaylayan
Ekrem MORAL Bilgi Güvenliği Yetkilisi	Erol ÖZTÜRK Personel ve Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Dr.Öğr.Üyesi Muhammet Ali ORUÇ İl Sağlık Müdürü