	UZAKTAN ERİŞİM PROSEDÜRÜ		T.C. SAĞLIK BAKANLIĞI AĞRI İL SAĞLIK MÜDÜRLÜĞÜ	
Kodu	**Yayınlama Tarihi**	**Revizyon Tarihi**	**Revizyon No**	**Sayfa**
KU.YÖ.01	17.12.2020	00	00	1

1. AMAÇ

Bu prosedürün amacı Bilgi Güvenliği kapsamında kurum ağında yer alan kaynaklara (sunucu, veri tabanı, servisler) uzaktan erişim için uyulması gereken kuralları anlatmak ve alınacak tedbirleri tanımlamaktır. Uzaktan erişimlerin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili erişimlerini sağlamaktır.

2. KAPSAM

Bu prosedür, Ağrı İl Sağlık Müdürlüğü ve bağlı sağlık tesislerindeki tüm bilgi varlıklarını, personelleri, Ağrı İl Sağlık Müdürlüğü ile bağlı tüm birim/sağlık tesislerine mal ve/veya hizmet sunan Yüklenici firmaları kapsamaktadır.

3. TANIMLAR

İSM: Ağrı İl Sağlık Müdürlüğü

SSL VPN: Secure Sockets Layer Virtual Private Network-Güvenli Yuva Katmanı Tabanlı Sanal Özel Ağ

4. PROSEDÜR METNİ

4.1.1. Uzaktan erişim için yalnızca SSL VPN uygulaması kullanılacak olup erişecek olan kullanıcı UZAKTAN ERİŞİM SÖZLEŞMESİ'ni doldurmak zorundadır.

4.1.2. Uzaktan erişim yöntemi olarak aşağıda açıklamaları verilen tünelleme, uygulama portalleri, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

- Tünelleme yöntemi, uzaktan çalışmada kullanılan bilgisayar ile iç ağın kriptolojik yöntemler kullanılmak suretiyle oluşturulan güvenli bir tünel vasıtasıyla birbirine bağlanmasıdır. Tünelleme işlemi, ağırlıklı olarak sanal özel ağ (VPN: Virtual Private Network) teknolojileri vasıtasıyla yapılır. VPN işlemi IP güvenliği (IPsec: IP Security), taşıma katmanı güvenliği (TLS: Transport Layer Security) veya güvenli kabuk (SSH: Secure Shell) protokolleri kullanılmak suretiyle yapılabilir.
- Uzak masaüstü erişim çözümleri, uzaktan çalışan kullanıcıların kurumun iç ağında yer alan bir sunucu veya istemci bilgisayarın karşısındaymış gibi kullanılmasını sağlar. Bu yöntemde, uzak kullanıcılar bağlanılan bilgisayarın klavye ve fare kontrollerini uzaktan yapar hale gelirler. Uzak masaüstü erişim yöntemleri kendi içlerinde birçok kısma ayrılır. Bazı erişim modellerinde vekil/terminal sunucu vasıtasıyla işlem yapılırken, bazı erişim modellerinde arada bir vekil/terminal sunucu olmadan da bağlantı kurulur.
- Doğrudan uygulama erişimlerinde, erişilecek uygulamalara ait sunucular kurumun halka açık sunucuların konumlandırıldığı "arındırılmış bölgeye (DMZ:De-Militarized Zone) yerleştirilir. Bu mimaride kullanıcılar genellikle web arayüzleri üzerinden doğrudan ilgili uygulama sunucusuna

Hazırlayan	Kontrol Eden	Onaylayan
Zeynep SAYGILI KARPUZ Bilgi Güvenliği Yetkilisi	Ahmet MAĞAL Kurumsal SOME Yetkilisi	Op. Dr. Coşkun DAHARLI İl Sağlık Müdürü

bağlanarak işlemlerini gerçekleştirirler. Doğrudan uygulama erişimleri genellikle daha az kritik uygulamalar için kullanılır. Bakanlığımızın güvenli metin aktarma iletişim protokolü (HTTPS: Secure Hyper Text Transfer Protocol) kullanılarak erişilebilen e-Posta (https://eposta.saglik.gov.tr) ve EBYS (https://www.ebys.saglik.gov.tr) sistemleri, yine hastanelerde laboratuvar tahlil sonuçlarının vatandaşlar tarafından doğrudan internet üzerinden sorgulanmasını sağlayan sistemler bu mimariye örnek olarak verilebilir.

- Portal uygulamaları, bir veya daha fazla uygulamanın genellikle web teknolojileri kullanılan tek bir arayüz üzerinden merkezi ve güvenli olarak sunulmasını sağlar. Portal çözümlerinde; portal sunucuları kurumun halka açık sunucuların konumlandırıldığı DMZ bölgesinde, uygulamalara ve veri tabanlarına ait sunucular ise iç ağa yerleştirilir. Bu şekilde uzaktan erişim yapacak kullanıcıların, uygulamalara ve verilere güvenli olarak erişmeleri sağlanır. Portal uygulamaları, doğrudan uygulama erişimlerinin özel bir türüdür.

4.1.3. Uzaktan erişim ile ilgili yöntem/mimari belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

- 6698 sayılı kanunun 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.
- VPN işlemi (bu maksatla kullanılan ayrı bir yazılım ve/veya donanım yoksa) İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.
- Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim "erişim yapacak kişi, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.
- VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.
- Uzaktan erişim için yetkilendirilmiş İSM ve\veya Bağlı Sağlık Tesisleri çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.
- Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.
- Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlanır. Bu süre 1 (bir) saati geçemez.

4.1.4. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

- Bağlantı SSL VPN üzerinden yapılır.
- Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.
- Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.
- Bağlantı yapan kullanıcının ağ üzerindeki hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.
- Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.
- Hedef bilgisayarda uzak bağlantı için kullanılan servis/arayüz vasıtasıyla, bilgisayara erişecek kullanıcılar "kullanıcı adı ve/veya IP adresi" bazında sınırlandırılır. Bu yöntemle sadece yetki verilen kullanıcıların/bilgisayarların uzaktan erişim yapması sağlanır.
- Microsoft işletim sistemi dışında bir başka bilgisayara erişim yapılıyorsa aynı güvenlik özelliklerini sağlayan, lisanslı ve/veya açık kaynak kodlu, güvenilir bir erişim programının kullanılması tercih edilir.

4.1.5. İnternet üzerinden İSM ve\veya Bağlı Sağlık Tesislerinin herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar SSL VPN teknolojisini kullanmalıdırlar.

4.1.6. SSL VPN Kullanıcı bilgileri, ihtiyaç olan İSM ve\veya Bağlı Sağlık Tesislerince ilgili kişi ve/veya kurumlara "SSL VPN Erişimi Talep Formu" ve "Personel Gizlilik Sözleşmesi" doldurtularak İSM'den talep edilmelidir.

4.1.7. İSM idaresince uygun görülen SSL VPN Kullanıcı talepleri İSM Sağlık Bilgi Sistemleri Birimince açılır ve bağlantı bilgileri sözlü\yazılı veya SSL VPN Erişimi Talep Formunda belirtilen e-posta adresi aracılığıyla ilgili kişilere bildirilir.

4.1.8. SSL VPN Kullanıcı şifresi İSM Parola Politikası ile uyumlu olmalıdır.

4.1.9. SSL VPN bağlantılarına ilişkin kayıtlar Bakanlığımız loglama sisteminde loglanmaktadır.

4.1.10. SSL VPN Kullanıcısı bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

4.1.11. İSM ve\veya Bağlı Sağlık Tesislerinden ilişiği kesilmiş veya görevi değişmiş kullanıcıların bilgileri ilgili sağlık tesisince İSM Sağlık Bilgi Sistemleri Birimine mümkün olan en kısa zamanda bildirilmeli ve Yetkili personelce ilgili kullanıcının yetki ve hesap özellikleri buna göre güncellenmelidir.

4.1.12. İSM ve\veya Bağlı Sağlık Tesisleri ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantıyı herkese açık güvenli olmayan alanlarda(kafeler, lokantalar, oteller vb.) yapmamalıdır.

4.1.13. Uzaktan erişim yaparken sahibi bilinmeyen/herkes tarafından erişilebilen cihazlar(internet kafe, otel bilgisayarları, kiosklar vb.) kullanılamaz.

4.1.14. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:

- Cihazlara kişisel güvenlik duvarı kurulur ve aktif halde olmalıdır.

- İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanmalıdır.
- Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı olmalıdır. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.
- Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.
- Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.
- Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.
- Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır. Disk şifreleme işlemleri için https://bilgiguvenligi.saglik.gov.tr/ adresinde yayımlanan sürücü şifreleme el kitaplarından yararlanılır.
- Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.
- Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.
- Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.
- Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için "jailbreak" veya "rootlama" işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.
- Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.
- Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

5. YAPTIRIM

Bu prosedürün ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan
Zeynep SAYGILI KARPUZ Bilgi Güvenliği Yetkilisi	Ahmet MAĞAL Kurumsal SÖME Yetkilisi	Op. Dr. Coşkun DAHARLI İl Sağlık Müdürü