

 T.C. Sağlık Bakanlığı	<b>UZAKTAN ERİŞİM PROSEDÜRÜ</b>			 T.C. Sağlık Bakanlığı
<b>Kodu</b>	<b>Yayınlanma Tarihi</b>	<b>Revizyon Tarihi</b>	<b>Revizyon No</b>	<b>Sayfa</b>
BG.PR.07	07.12.2018			1 / 1

## 1. AMAÇ

- 1.1.1. 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.


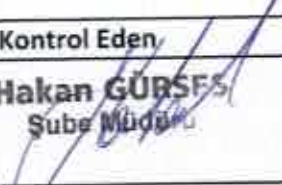
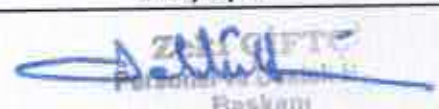
## 2. KAPSAM

- 2.1.1. Bu prosedür, İl Sağlık Müdürlüğü ve bağlı sağlık tesislerindeki personelleri, kurumlara mal ve/veya hizmet sunan Yüklenici firmaları kapsamaktadır.

## 3. TANIMLAR

## 4. PROSEDÜR METNİ

- 4.1.1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
- 4.1.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.
- 4.1.3. 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. Daha fazlası için parola politikasına bakınız.
- 4.1.4. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
- 4.1.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
- 4.1.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
- 4.1.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
- 4.1.8. Kurumdan ilişkisi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
- 4.1.9. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.
- 4.1.10. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
- 4.1.11. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.
- 4.1.12. VPN ile erişecek olan kullanıcı UZAKTEN ERİŞİM FORMU'nu doldurmak zorundadır.
- 4.1.13. Uzak erişim bağlantısında boştaki kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
 Hakan DEMİR Bilgi İşlem	 Hakan GÜRSER Şube Müdürü	 Zekiye ÇETİ Personel ve Eğitim Başkanı