



| Kodu         | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|--------------|------------------|-----------------|-------------|-------|
| PDH.BG.PR.09 |                  |                 | --          |       |

## 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.

## 2. KAPSAM

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

## 3. UYGULAMA METNİ

- Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
- 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.
- 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.
- Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
- Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
- Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.



| Kodu         | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|--------------|------------------|-----------------|-------------|-------|
| PDH.BG.PR.09 |                  |                 | --          |       |

- 7) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
- 8) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
- 9) Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.
- 10) Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
- 11) Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.
- 12) VPN ile erişecek olan kullanıcı UZAKTEN ERİŞİM FORMU'nu doldurmak zorundadır.
- 13) Uzak erişim bağlantısında boшта kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.