



T.C. SAĞLIK BAKANLIĞI

UZAKTAN ERİŞİM PROSEDÜRÜ



T.C. SAĞLIK BAKANLIĞI
KAYSERİ
İL SAĞLIK MÜDÜRLÜĞÜ

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

3. UYGULAMA

- 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. 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.
- Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
- Kurumdan ilişkisi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
- Uzak erişimde yapılan tüm network hareketleri log'lanmalıdır.
- Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
- Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.
- Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.