## 1. AMAÇ

Bu prosedürün amacı, T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri/Birimleri bünyesinde yer alan kaynaklara uzaktan erişim için bilgi güvenliği kapsamında uyulması gereken kuralları tanımlamaktır.

## 2. KAPSAM

Bu Prosedür, T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri/Birim çalışanları ile kuruma mal veya hizmet sunan ve kurumun bilgi varlıklarına uzaktan erişen yüklenici-tedarikçi gibi geçici olarak iş ilişkisi olan firmaları kapsar.

## 3. TANIMLAR

**Uzaktan Çalışma:** 4857 sayılı İş Kanununun 14'üncü maddesine göre; "çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi" olarak tanımlanmaktadır.

**VPN:** Sanal Özel Ağ

**SBA:** Sağlık Bilişim Ağı

**Muhtemel uzak çalışma ortamları şunlardır:**

-T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğüne ait ancak SBA bağlantısı olmayan yerler (aktif cihaz sayısı 10'dan az olan müstakil bina ve tesisler),

-Çalışanların evleri veya (tedarikçiler, iş ortakları için) ofisleri,

-Herkese açık alanlar (kafeler, lokantalar, oteller vb.),

- T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğü ve bağlı birimlerin fiziki ortamını kullanan ancak kurum ağına (SBA'ya) doğrudan bağlanma izni verilmeyen durumlar (örneğin; kurum tesislerinde çalışan yüklenici personeli, kendi cihazları ile kurumun diğer ağlarına bağlanan çalışanlar).

## 4. UYGULAMA

**Dikkat edilecek hususlar:**

-Uzaktan erişim yöntemi olarak tünelleme, uygulama portalleri, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılır.

| Hazırlayan | Onaylayan |
|---|---|
| Suat SAĞLAM<br>Bilgi Güvenliği Yetkilisi | Dr.Mehmet Hakan PAMUKÇU<br>İl Sağlık Müdürü |

-Tünelleme işlemi ve masaüstü erişimleri VPN (IPSec, TLS,SSH) teknolojileri vasıtasıyla yapılır.
-VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.
-Uzak çalışmalar için hangi uzak erişim yönteminin veya yöntemlerinin kullanılacağına, risk değerlendirmesine bağlı olarak ihtiyacı karşılayabilecek ve risk düzeyi düşük olana göre karar verilir.
-Özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılır.
-VPN işlemi İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.
-Hedef bilgisayarlara sabit IP adresi verilir.
-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) 1 saati geçmemelidir.
-Uzak masaüstü erişimlerde, 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.
-Uzak masaüstü erişimlerde uzak bağlantı yazılımı olarak mümkün ise “Microsoft Uzak Bağlantı Programı” kullanılır.
-Uzaktan çalışma için T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğü ve bağlı birimlerine ait cihazlar kullanılır.
-Uzaktan çalışacak kişi T.C Sağlık Bakanlığı Batman İl Sağlık Müdürlüğü ve bağlı birimleri ile sözleşme/protokol imzalayan üçüncü taraf personeli ise ve kuruma ait bilgisayar verilemiyorsa, uzak çalışma için hangi tip cihazlar kullanılacağı ve bu cihazlarda alınması gereken tedbirler, ilgili sözleşme/protokollere konulur.
-Uzak masaüstü bağlantısında, şahısların kendilerine ait kişisel cihazlar veya sahibi bilinmeyen/herkes tarafından erişilebilen terminaller kullanılmaz. Kullanıcıların bu tip terminaller üzerinden uzak masaüstü bağlantısı yaptıklarının tespit edilmesi halinde gerekli yasal ve idari yaptırımlar uygulanır.
-Uzaktan çalışmanın hiçbir çeşidinde sahibi bilinmeyen/herkes tarafından erişilebilen (internet kafe, otel bilgisayarları, kiosklar vb.) kullanılmaz.
-Uzak çalışmada kullanılacak cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.
-İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamaları için otomatik güncelleme seçilerek güncel halde tutulması sağlanır.
-Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı tedarik edilir. 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 vb.) pasif hale getirilir.
-Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.
-“jailbreak” veya “rootlama” işlemi yapılan 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.

| Hazırlayan | Onaylayan |
|---|---|
| Suat SAĞLAM<br>Bilgi Güvenliği Yetkilisi | Dr.Mehmet Hakan PAMUKÇU<br>İl Sağlık Müdürü |