T.C.
DENİZLİ VALİLİĞİ
İL SAĞLIK MÜDÜRLÜĞÜ
UZAKTAN ERİŞİM PROSEDÜRÜ

1. AMAÇ

Müdürlüğümüz ve Bağlı Sağlık Tesislerine bünyesindeki bilgi kaynaklarına(sunucu ve hizmetlere) uzaktan erişim için alınması gereken tedbirler ve uyulması gereken kuralları açıklamaktır.

2. KAPSAM

Denizli İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesislerinde çalışan ve/veya sözleşme ile yüklenici, tedarikçi, iş ortakları kapsamında olup uzaktan bağlantı yapması gereken tüm çalışanları kapsar.

3. TANIMLAR

İSM: Denizli İl Sağlık Müdürlüğü

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

4. SORUMLULUKLAR

Bu prosedürün uygulanmasından ilgili kurum yöneticileri sorumludur.

5. UYGULAMA

5.1. Uzaktan Erişim Prosedürü

5.1.1. 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.

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

5.1.3. 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.

5.1.4. 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.

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

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

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

5.1.8. 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.

5.1.9. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

5.1.9.1. Bağlantı SSL VPN üzerinden yapılır.

5.1.9.2. Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.

5.1.9.3. Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.

5.1.9.4. Bağlantı yapan kullanıcının ağ üzerindeki hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.

5.1.9.5. Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.

5.1.9.6. 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.
5.1.10. 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.
5.1.11. Uzaktan erişim yaparken sahibi bilinmeyen/herkes tarafından erişilebilen cihazlar(internet kafe, otel bilgisayarları, kiosklar vb.) kullanılamaz
5.1.12. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:
5.1.12.1. Cihazlara kişisel güvenlik duvarı kurulur ve aktif halde olmalıdır.
5.1.12.2.İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanmalıdır.
5.1.12.3. Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı olmalıdır. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.
5.1.12.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.
5.1.12.5. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.
5.1.12.6. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.
5.1.12.7. 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.
5.1.12.8. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.
5.1.12.9. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.
5.1.12.10. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.
5.1.12.11. Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için “jailbreak” veya “rootlama” işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.
5.1.12.12. Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.
5.1.12.13. Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

6. 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.