1. AMAÇ

Bu prosedürün amacı, S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi faaliyetlerinin belirlenen politika, prosedür ve diğer bilgi güvenliği gereklilikleri çerçevesinde yürütülmesini, ayrıca Bilgi Güvenliği Yönetim Sistemi (BGYS)' nin sürekli iyileştirilmesini sağlamak ve belirlenen hedeflere ulaşmak amacıyla uzaktan erişimlerin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili kullanıcıların erişimlerini sağlamaktır.

2. KAPSAM

Bu prosedür S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde bulunan sistemlere BGYS kapsamında uzaktan erişimi gerçekleştirecek tüm iş ve işlemleri kapsamaktadır.

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.

4. UYGULAMA

4.1. Uzaktan çalışma; ağırlıklı olarak yükleniciler, tedarikçiler, iş ortakları çalışanları gibi İl Sağlık Müdürlüğümüz ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır. Ancak acil durumlarda S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi çalışanları için de söz konusu olabilir.

4.2. Uzaktan çalışma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliğini sağlamak için ek önlemler alınması gerekir.

4.3. Uzaktan çalışma ile ilgili kontrol tedbirleri belirlenirken aşağıda sıralanan dört temel tehdit unsuru/modeli dikkate alınır.

4.3.1. Uzak çalışma ortamlarının fiziki güvenliğindeki yetersizlikler,
4.3.2. Uzak bağlantının güvenli olmayan ağ ortamları (çoğunlukla internet) üzerinden yapılması,
4.3.3. Kurum güvenlik politikaları uygulanmamış güvenilir olmayan cihazların iç ağa bağlanması,
4.3.4. İç ağdaki kaynaklara dışarıdan erişim.

4.4. Günümüzde teknolojinin bizlere sağlamış olduğu yetenekler kullanılmak suretiyle, farklı yön- temler kullanılarak uzak bağlantı yapılması mümkündür.

4.5. Uzaktan erişim için en uygun yöntemin belirlenmesi amacıyla, her ihtiyacın kendine özgü şartları ve risklerinin ayrıntılı olarak değerlendirilmesi gerekir.

Hazırlayan	Kontrol Eden	Onaylayan

4.6. Uzaktan erişim yöntemi olarak aşağıda açıklamaları verilen tünelleme, uygulama portalleri, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

4.7. Uzaktan erişim ile ilgili yöntem/mimari belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

4.7.1. Bakanlığımızda genel bir politika olarak uzak masaüstü işlemleri VPN bağlantısı üzerinden yapılır. VPN bağlantısı yapılmadan doğrudan uzak masaüstü bağlantısı yapılmasına hiçbir şekilde izin verilmez.

4.7.2. 6698 sayılı kanunun açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

4.7.3. VPN işlemi (bu maksatla kullanılan ayrı bir yazılım ve/veya donanım yoksa) İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.

4.7.4. Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim "erişim yapacak kişi, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.

4.7.5. VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.

4.7.6. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.

4.7.7. Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.

4.7.8. Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlanır. Bu süre 1 (bir) saati geçemez.

4.7.9. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

4.7.9.1. Bağlantı VPN üzerinden yapılır.

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

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

4.7.9.4. 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.

4.7.9.5. Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.

Hazırlayan	Kontrol Eden	Onaylayan

4.7.9.6. Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise (örneğin SBYS yazılımı kullanılacak ise) ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları da kayıt altına alınır.

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

4.7.9.8. 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.

4.8. Uzaktan çalışma için kullanılacak cihazlar belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

4.8.1. Uzaktan çalışma prensip olarak S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi birimlerine ait cihazlar ile yapılır.

4.8.2. Uzaktan çalışacak kişi S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi 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. Bu maksatla kullanılacak cihazlara ait bilgiler kuruma resmi olarak bildirilir. Kurum tarafından üçüncü taraflarda yapılacak denetimlerde belirtilen işlemlerin yapılıp yapılmadığı aranır.

4.8.3. Uzak çalışma kapsamında uzak masaüstü bağlantısı yapılacaksa, 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.

4.8.4. Doğrudan uygulama erişimleri de dâhil uzaktan çalışmanın hiçbir çeşidinde sahibi bilinmeyen/herkes tarafından erişilebilen (internet kafe, otel bilgisayarları, kiosklar vb.) kullanılmaz.

4.8.5. Uzaktan çalışma için kullanılacak cihazlarda S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi ait gizlilik dereceli bilgiler depolanacak ise bahse konu verilerin şifreli olarak saklanmasına imkân verecek, tercihan işlemci gücü yüksek bilgisayarlar kullanılır.

4.9. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:

4.9.1. Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.

4.9.2. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanır.

4.9.3. 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.

4.9.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.

Hazırlayan	Kontrol Eden	Onaylayan

4.9.5. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.

4.9.6. Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.

4.9.7. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.

4.9.8. 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.

4.9.9. Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.

4.9.10. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.

4.9.11. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.

4.9.12. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.

4.9.13. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

4.9.14. Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.

4.9.15. Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

Hazırlayan	Kontrol Eden	Onaylayan