



TASNİF DIŐI
UZAKTAN ÇALIŐMA VE ERİŐİM PROSEDÜRÜ



T.C. SAĐLIK BAKANLIĐI
SAĐLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĐÜ

| Kodu | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|----------|------------------|-----------------|-------------|-------|
| BG.PR.35 | 15.12.2018 | 24.07.2020 | 1 | 1 / 4 |

1. AMAÇ

Bu prosedür, **BG.PO.24 EriŐim Politikası** uyarınca yapılacak uzaktan çalıŐma ve uzaktan eriŐim ile ilgili süreçleri düzenlemek üzere hazırlanmıŐtır.

2. KAPSAM

Bu prosedür, Genel Müdürlüğümüzde görev yapan tüm çalıŐanları, ayrıca Genel Müdürlüğümüz tarafından iŐletilen sunucu ve sistemlere bağlanarak uzaktan çalıŐma ve uzaktan eriŐim yapan tüm gerçek kişileri kapsar.

3. UYGULAMA

3.1 Uzaktan ÇalıŐma:

3.1.1 Uzaktan çalıŐma 4857 sayılı İŐ Kanununda **çalıŐanların, iŐveren tarafından oluşturulan iŐ organizasyonu kapsamında, iŐ görme edimini evinde ya da teknolojik iletiŐim araçları ile iŐyeri dıŐında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iŐ iliŐkisi** olarak tanımlanmıŐtır.

3.1.2 Uzaktan çalıŐma; yükleniciler, tedarikçiler, iŐ ortakları çalıŐanları gibi Genel Müdürlüğümüz ile geçici olarak iŐ iliŐkisi olan kişiler tarafından yapılır. Ancak

- Dođal afet, salgın hastalık gibi olađanüstü hallerde yetkili makamlar tarafından uygun görüldüđü durumlarda,
- Verilen bir görevin acil olarak yerine getirilmesi veya iŐletilmekte olan sunucu ve sistemlere **7*24** esasına göre uzaktan destek verilmesi gereken durumlarda,
- İl dıŐı görevlendirme vb. nedenlerle kurum dıŐında çalıŐılması gereken durumlarda **Genel Müdürlüğümüz personeli tarafından da “uzaktan çalıŐma” yapabilir.**

3.1.3 Uzaktan çalıŐma iŐlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliđinin sađlanması için ek önlemler alınır.

3.1.4 Genel Müdürlüğümüz çalıŐanları, uzaktan çalıŐma için Kurum tarafından verilen bilgisayarları kullanmak zorundadır. Ancak “iŐ sürekliliđinin sađlanması, iŐletilmekte olan sunucu ve sistemlere uzaktan destek verilmesi” gibi çok acil hallerde, başka bir imkân olmadıđı için şahsi bilgisayarların kullanılması durumunda, kurumsal verilerin söz konusu bilgisayara indirilmemesi ve iŐlenmemesi için gerekli özen gösterilir. Yapılan müdahalenin dođası geređi bilgisayara indirilen verilerin güvenli olarak silinmesi, iŐlemi gerçekteŐtiren kişilerin sorumluluđundadır.

3.1.5 Uzaktan çalıŐma yapacak kişiler, Genel Müdürlüğümüz ile sözleşme/protokol imzalayan üçüncü taraf personeli ise ve bu kişilere kuruma ait bilgisayar verilemiyorsa; uzaktan çalıŐma esnasında kullanılacak cihazlarda gerekli güvenlik tedbirlerinin alınması, **BG.SZ.01 Personel Gizlilik Sözleşmesi** ve **BG.SZ.02 Kurumsal Gizlilik Taahhütnamesi** uyarınca ilgili kişilerin ve çalıŐanı oldukları firma/kurumun tüzel kişiliđinin sorumluluđundadır. Bu kapsamda Bakanlığımıza ait gizlilik dereceli bilgilerin söz konusu bilgisayarlarda **BG.PR.14 Kriptografik Kontroller ve Anahtar Yönetimi Prosedüründe** belirtilen yöntemlerle şifreli olarak saklanması, kullanımına ihtiyaç olmayan verilerin güvenli silme araçları ile kalıcı olarak silinmesi gerekmektedir.

| Hazırlayan | Kontrol Eden | Onaylayan |
|--|--|--|
| Gamze CİMİLLİ Altyapı Yatırım, EriŐim ve Yetkilendirme Koordinasyon Birimi Birim Sorumlusu | Erdal YILDIZ Bilgi Güvenliđi Yönetim Sistemleri Birimi/ Bilgi Güvenliđi DanıŐmanı | M. Fatih ULUÇAM Sistem Yönetimi ve Bilgi Güvenliđi Daire BaŐkanı / Yönetim Temsilci |



TASNİF DIŐI
UZAKTAN ÇALIŐMA VE ERİŐİM PROSEDÜRÜ



T.C. SAĐLIK BAKANLIĐI
SAĐLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĐÜ

| Kodu | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|----------|------------------|-----------------|-------------|-------|
| BG.PR.35 | 15.12.2018 | 24.07.2020 | 1 | 2 / 4 |

3.1.6 Bakanlık web tabanlı e-posta sistemi, EBYS, ÇKYS, kurumsal portal gibi doğrudan uygulama erişimleri de dâhil olmak üzere uzaktan çalışmanın hiçbir çeşidinde, sahibi bilinmeyen/herkes tarafından erişilebilen internet kafe, otel bilgisayarları, kiosk vb. ortamlar kullanılamaz. Kullanıcıların bu tip terminaller üzerinden Bakanlığımız sistemlerine bağlantı yaptıklarının tespit edilmesi halinde **BG.PR.06 BGYS Disiplin Prosedüründe** belirtilen yaptırımlar uygulanır.

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

3.2.1 Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.

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

3.2.3 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.

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

3.2.5 Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlemesi sağlanır.

3.2.6 Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise "dizüstü bilgisayar kilidi ve güvenlik kablosu" kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.

3.2.7 Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (Wi-Fi, Bluetooth vb.) pasif hale getirilir.

3.2.8 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.

3.2.9 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.

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

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

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

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

| Hazırlayan | Kontrol Eden | Onaylayan |
|--|--|--|
| Gamze CİMİLLİ Altyapı Yatırım, Erişim ve Yetkilendirme Koordinasyon Birimi Birim Sorumlusu | Erdal YILDIZ Bilgi Güvenliği Yönetim Sistemleri Birimi/ Bilgi Güvenliği Danışmanı | M. Fatih ULUÇAM Sistem Yönetimi ve Bilgi Güvenliği Daire Başkanı / Yönetim Temsilci |



TASNİF DIŐI
UZAKTAN ÇALIŐMA VE ERİŐİM PROSEDÜRÜ



T.C. SAĐLIK BAKANLIĐI
SAĐLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĐÜ

| Kodu | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|----------|------------------|-----------------|-------------|-------|
| BG.PR.35 | 15.12.2018 | 24.07.2020 | 1 | 3 / 4 |

3.2.14 Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için "jailbreak" veya "rootlama" işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

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

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

3.3 Uzaktan Erişim

3.3.1 Uzaktan çalışma yapacak kullanıcıların Genel Müdürlüğümüz tarafından işletilen ve özel koruma gerektiren bilişim kaynaklarına (sunucu ve ağ cihazlarının yönetim panelleri, VTYS yönetim arayüzleri, kritik uygulamalar vb.) erişimi, VPN (sanal özel ağ) bağlantısı üzerinden gerçekleştirilir.

3.3.2 Kişilere VPN erişimi verilebilmesi için;

- o Devlet memurları, diğer kamu görevlileri (sürekli işçiler ve sözleşmeli bilişim personeli) ve Dünya Bankası danışmanları için **BG.FR.67 VPN Hesabı Açılacak Kamu Personeli İçin Bilgi Formunun**,
- o Firma personeli için ilgili kişilerin **BG.SZ.01 Personel Gizlilik Sözleşmelerinin**,
- o Erişim verilecek kişiler bir firma veya Bakanlığımız dışında bir başka kurumun çalışanı ise ilgili firma/kuruma ait **BG.SZ.02 Kurumsal Gizlilik Taahhünamesinin**,
- o Bağlantı ihtiyacına ilişkin detaylı açıklamaların (ihtiyacın gerekçesi, erişilmek istenen bilişim kaynakları) resmi yazı ile Genel Müdürlüğümüze (Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığına) gönderilmiş olması gerekir.

3.3.3 VPN erişim talepleri, Genel Müdürlüğümüzün ilgili birimleri tarafından detaylı olarak incelenir. Gerekirse erişilecek bilişim kaynağının sahiplerinden doğrulama yapılır. İhtiyaç olması halinde ilave bilgi ve belge istenebilir.

3.3.4 Erişim talebinin uygun görülmesi halinde, ilgili bilgi ve belgeler Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığında görev yapan personel tarafından <https://sozlesme.saglik.gov.tr/> uygulamasına girilir.

3.3.5 VPN erişimlerinde iki kademeli kimlik doğrulama yapılır. Bu kapsamda, ilk kademede <https://sslvpn.saglik.gov.tr/> adresinden kimlik bilgileri ve parolanın sisteme doğru bir şekilde girilmesi; ikinci aşamada SMS veya TOKEN kullanmak suretiyle kişinin kimliğinin bir başka araç üzerinden yeniden doğrulanması gerekir.

3.3.6 VPN bağlantısının yapılması aşamasında dikkat edilecek hususlar, **BG.TL.04 VPN Erişimi Kurulum ve Kullanım Talimatında** açıklanmıştır. Talimata <https://bilgiguvenligi.saglik.gov.tr/Home/Dokumantasyon> adresinden erişim sağlanabilir.

3.3.7 VPN erişimi yapan kullanıcıların erişim yaptıkları kaynaklar üzerinde yaptıkları işlemler, "Yetkili Kullanıcı Hesap Yönetim Sistemi" tarafından video ve/veya metin (text) formatında kayıt altına alınır.

| Hazırlayan | Kontrol Eden | Onaylayan |
|--|--|--|
| Gamze CİMİLLİ Altyapı Yatırım, Erişim ve Yetkilendirme Koordinasyon Birimi Birim Sorumlusu | Erdal YILDIZ Bilgi Güvenliği Yönetim Sistemleri Birimi/ Bilgi Güvenliği Danışmanı | M. Fatih ULUÇAM Sistem Yönetimi ve Bilgi Güvenliği Daire Başkanı / Yönetim Temsilci |



TASNİF DIŐI
UZAKTAN ÇALIŐMA VE ERİŐİM PROSEDÜRÜ



T.C. SAĐLIK BAKANLIĐI
SAĐLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĐÜ

| Kodu | Yayınlama tarihi | Revizyon Tarihi | Revizyon No | Sayfa |
|----------|------------------|-----------------|-------------|-------|
| BG.PR.35 | 15.12.2018 | 24.07.2020 | 1 | 4 / 4 |

3.3.8 VPN erişimleri altı aylık süre sonunda otomatik olarak askıya alınacak şekilde verilir. Altı aylık sürenin sonunda ilgili kişinin Genel Müdürlüğümüz/Bakanlığımız ile ilişkisinin devam edip etmediđi e-posta veya resmi yazı ile teyit edilir. Kişinin çalışmaya devam ettiđinin teyit edilmesi halinde, sözleşmesinde belirtilen süre dikkate alınarak erişim izni uzatılır.

3.3.9 İlgili kişinin BG.SZ.01 Personel Gizlilik Sözleşmesinde yazan “**Sözleşme Geçerlilik Tarihi**”nin dolması durumunda, altı aylık sürenin dolmasını beklemeksizin erişimi askıya alınır. Kişiyeniden erişim izni verilebilmesi için **3.3.2 maddesinde belirtilen sürecin** yenilenmesi gerekir.

4. YAPTIRIM

Bu politikanın ihlali durumunda **BG.PR.06 BGYS Disiplin Prosedüründe** belirtilen yaptırımlar uygulanır.

5. DOKÜMANLAR

BG.FR.67 VPN HESABI AÇILACAK KAMU PERSONELİ İÇİN BİLGİ FORMU

BG.PO.24 ERİŐİM POLİTİKASI

BG.PR.14 KRİPTOGRAFİK KONTROLLER VE ANAHTAR YÖNETİMİ PROSEDÜRÜ

BG.PR.06 BGYS DİŐİPLİN PROSEDÜRÜ

BG.SZ.01 PERSONEL GİZLİLİK SÖZLEŐMESİ

BG.SZ.02 KURUMSAL GİZLİLİK TAAHHÜTNAMESİ

BG.TL.04 VPN ERİŐİMİ KURULUM VE KULLANIM TALİMATI

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Gamze CİMİLLİ Altyapı Yatırım, EriŐim ve Yetkilendirme Koordinasyon Birimi Birim Sorumlusu | Erdal YILDIZ Bilgi Güvenliđi Yönetim Sistemleri Birimi/ Bilgi Güvenliđi DanıŐmanı | M. Fatih ULUÇAM Sistem Yönetimi ve Bilgi Güvenliđi Daire BaŐkanı / Yönetim Temsilci |