



**UZAKTAN ÇALIŞMA  
POLİTİKASI**

<b>Doküman No</b>	BİD.BGYS.PT-0003
<b>Yayın Tarihi</b>	06.02.2023
<b>Revizyon Tarihi</b>	00.00.0000
<b>Revizyon No</b>	00
<b>Sayfa No</b>	1/7

**GAZİ ÜNİVERSİTESİ**  
**BİLGİ İŞLEM DAİRE BAŞKANLIĞI**

*UZAKTAN ÇALIŞMA POLİTİKASI*

1926



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	2/7

### Revizyon Tarihçesi

Revizyon No	Revizyon Gerekçesi	Revizyon Tarihi

HAZIRLAYAN  
BGYS SORUMLUSU

ONAYLAYAN  
BİLGİ İŞLEM DAİRE BAŞKANI



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	3/7

### İçindekiler Tablosu

1. AMAÇ .....	4
2. KAPSAM .....	4
3. TANIMLAR VE KISALTMALAR .....	4
4. UYGULAMA .....	4
4.1. Uzaktan Çalışma ile İlgili Temel Prensipler .....	4
4.2. Video Konferans ile İlgili Temel Prensipler .....	5
4.3. Kurum Dışı Personel için Uzaktan Çalışma ile İlgili Temel Prensipler .....	6
4.4. Uzaktan Çalışma Talepleri .....	6
5. YAPTIRIM VE CEZA .....	6
6. GÖZDEN GEÇİRME VE ONAY .....	7
7. İLGİLİ DÖKÜMANLAR .....	7

HAZIRLAYAN  
BGYS SORUMLUSU

ONAYLAYAN  
BİLGİ İŞLEM DAİRE BAŞKANI



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	4/7

### 1. AMAÇ

Bu politika, uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak ve bilgi güvenliği kapsamında uyulması gereken kuralları tanımlamak amacıyla oluşturulmuştur.

### 2. KAPSAM

Bu politika, Gazi Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde çalışanları ile kuruma destek hizmeti veren ve kurumun bilgi varlıklarına uzaktan erişen tüm bileşenleri kapsamaktadır.

### 3. TANIMLAR VE KISALTMALAR

<b>Kurum</b>	Gazi Üniversitesi
<b>BİDB</b>	Bilgi İşlem Daire Başkanlığı
<b>BGYS</b>	Bilgi Güvenliği Yönetim Sistemi
<b>Kullanıcı</b>	Kurumsal Bilgiye Erişen Kişi
<b>VPN</b>	Sanal Özel Ağ
<b>Uzaktan Çalışma</b>	4857 sayılı İş Kanunu'nun 14'üncü maddesine göre; "çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini 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 ile İlgili Temel Prensipler

- Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ve kimlik doğrulama ile sağlanır.
- Uzaktan çalışma için kişisel cihazların kullanımına izin verilmesi durumlarında personel Varlıkların Kabul Edilebilir Kullanımı Politikası ile Mobil Cihaz Politikası'na uygun olarak hareket eder.
- Uzaktan erişim için tanımlanacak tüm kullanıcı hesapları, yetkiler ve parolaları Parola ve Şifreleme Politikasına uyumlu şekilde yönetilir.
- VPN bağlantısı gerçekleştirilecek cihazın işletim sistemi güncel ve lisanslı olmalıdır.
- VPN bağlantısı gerçekleştirecek cihazda lisanslı ve güncel bir antivirüs çözümünün kullanılması gerekmektedir.
- Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar

HAZIRLAYAN BGYS SORUMLUSU	ONAYLAYAN BİLGİ İŞLEM DAİRE BAŞKANI
------------------------------	--



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	5/7

kullanılır. Örneğin, kişisel e-posta hesapları kullanılamaz.

- Uzaktan çalışan kurum personeli, uzaktan çalışma talebi yaparken uzaktan çalışmanın getirdiği risklere karşı uyarılır, bunun için VPN Talep Formu'nda yer alan bilgileri okuması ve kabul etmesi sağlanır.
- Uzaktan çalışma alanının güvenli olmasına dikkat edilir, bina ve çevrenin fiziksel güvenliği dikkate alınarak sağlanır.
- Uzaktan çalışma esnasında güvenilirliğinden emin olunan, sahibi bilinen ağ, sistem ve cihazlar kullanılır.
- Cihazın fiziksel olarak güvenliği emniyet altına alınır.
- Aynı ikametgahı kullanan aile ve arkadaşlar gibi kişiler tarafından kurumsal bilgi ve kaynaklara yetkisiz erişim tehdidine karşı gereken önlemler **Varlıkların Kabul Edilebilir Kullanımı Politikası**'na göre alınır.
- Uzaktan çalışılırken sahibi bilinmeyen veya herkes tarafından erişilebilen (internet kafe, otel bilgisayar, ortak ağlar, kiosklar vb.) ağ, sistem ve cihazlar hiçbir şekilde kullanılmaz.
- Uzaktan erişim, çift faktörlü bir kimlik doğrulama sonucunda gerçekleşir. Kullanıcı adı ve parolaya ek olarak çift faktörlü erişim metodlarından bir veya birkaç tanesi (Authenticator, SMS, OTP vb.) kullanılmalıdır.
- Uzaktan erişimler güvenli bir algoritma kullanan kriptolu bir tünel bağlantısı (SSL VPN, IPSec VPN) aracılığıyla gerçekleştirilir.
- Cihazlarda güvenlik duvarı aktif hale getirilir.
- Tüm uzaktan erişim işlemleri için oturum kayıtları LOG Yönetimi Planına göre tutulur ve 2 yıl saklanır. Bu kayıtlarda oturum açma (login) ve oturum kapama (logout) bilgileri tutulur.
- VPN cihazına ait olay kayıtları tutulur, SIEM üzerinde izlenir.
- Cihaza ekran koruma süresi konularak (30 dakika) işlem yapılmadığında oturumun otomatik olarak kapatılması sağlanır.
- Uzaktan masaüstü erişimi üzerinde oturum kontrolü bulunur. Aynı anda bir kullanıcı hesabıyla iki farklı bağlantıya izin verilmez.
- Yetkili kullanıcıların uzaktan erişim için kullandığı bilgisayarlarda iz kalması engellenir, bu amaçla çerez ve sayfa önbellek ayarları kullanıcı oturumunun veya kritik bilgilerin çalınmasını ve taklit edilmesini engelleyecek şekilde yapılandırılır.

### 4.2. Video Konferans ile İlgili Temel Prensipler

- Video konferans kurumun onayladığı güvenilir bir platform üzerinden gerçekleştirilebilir.
- Video konferans görüşmelerine sadece toplantı bağlantı adresi kullanılarak yapılabilecek yetersiz erişimlerin engellenmesi sağlanır.

HAZIRLAYAN BGYS SORUMLUSU	ONAYLAYAN BİLGİ İŞLEM DAİRE BAŞKANI
------------------------------	--



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	6/7

### 4.3. Kurum Dışı Personel için Uzaktan Çalışma ile İlgili Temel Prensipler

- VPN erişimleri VPN Talep Formunda belirtilen süreyi geçemez. Süre bitiminde ihtiyaç duyulursa yeniden talep oluşturulur.
- Gerekli görüldüğü durumlarda bağlantı sırasında yapılan işlemler kayıt altına alınabilir.
- Kurum personeli, erişim başladıktan sonra ekranı ve yapılan işlemleri takip eder.
- Yapılan işlemlerin kritiklik seviyesine göre bağlantı yapan kişinin oturum kayıtları yanı sıra eriştiği sistemi ve yapılan işlemlerin görüntüleri veya sisteme verilen komutların logları çeşitli yazılımlar aracılığı ile tutulabilir.

### 4.4. Uzaktan Çalışma Talepleri

- Uzaktan erişim yapacak kurum personeli, VPN Talep Formunu doldurur. Sonrasında birim amirine onaylatılan form tanımlamaları yapacak olan Sistem Yöneticisine iletilir.
- Uzaktan erişim yapacak olan kişi kurum dışından bir çalışan ise Frm.04-Rev.00-Tarafsızlık ve Gizlilik Beyanı imzalatılır ve VPN talep formu doldurtulur. Birim amirine onaylatılan form tanımlamaları yapacak olan Sistem Yöneticisine iletilir. Bu işlemler EBYS sistemi üzerinden gerçekleştirilebilir.
- Uzaktan erişim yenilemeleri, “VPN Güncelleme Formu” doldurtularak ilk defa tanımlanan uzaktan erişimler ile aynı aşamalardan ve onaylardan geçerek gerçekleştirilir.
- Erişim süresi başlangıç tarihinden itibaren en fazla 1 yıl olup bu süre sonunda erişim otomatik olarak pasif hale getirilecektir. Devam etmesi istenen erişimler için erişim sonlandırılmadan önce “VPN Güncelleme Formu” doldurularak tekrar talepte bulunulması gerekmektedir.

## 5. YAPTIRIM VE CEZA

Tüm kullanıcılar **uzaktan çalışma politikası** ile birlikte; BGYS kapsamındaki tüm ilgili politika ve prosedürlerdeki kuralları bilmek ve bu kurallara uymaktan, bilgi varlıklarına erişim hakkı istemek için kurum tarafından onaylanmış süreç ve prosedürleri kullanmaktan, şifre, e-imza gibi kurum tarafından verilmiş olan kimlik doğrulama bilgilerini korumaktan, bilgi kendi kullanımındayken bilginin gizliliğini, bütünlüğünü ve erişebilirliğini varlık sahibi tarafından belirlenen önlemlere uygun olarak korumaktan sorumludur. **Uzaktan çalışma politikası** tarafından düzenlenen kurallara uymayanlara Disiplin Prosedürü çerçevesinde yaptırım ve cezalar uygulanır. Bu cezalar 657 sayılı Devlet Memurları Kanunu ve kişinin bağlı olduğu ilgili diğer mevzuatlara uygun olarak belirlenir.

HAZIRLAYAN  
BGYS SORUMLUSU

ONAYLAYAN  
BİLGİ İŞLEM DAİRE BAŞKANI



## UZAKTAN ÇALIŞMA POLİTİKASI

Doküman No	BİD.BGYS.PT-0003
Yayın Tarihi	06.02.2023
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa No	7/7

### 6. GÖZDEN GEÇİRME VE ONAY

**Uzaktan Çalışma Politikası** yılda bir kez BGYS Birimi koordinesinde gözden geçirilir ve varsa değişiklikler Bilgi İşlem Daire Başkanı tarafından onaylanır. Gözden geçirme, Yönetimin Sistemi Gözden Geçirme Toplantısı gündemine alınarak gerçekleştirilir.

### 7. İLGİLİ DÖKÜMANLAR

- Varlıkların Kabul Edilebilir Kullanımı Politikası
- Mobil Cihaz Politikası
- Parola ve Şifreleme Politikası
- LOG Yönetimi Planı
- Fr.0046-Rev.01-VPN Talep Formu
- Fr.0055-Rev.00-VPN Güncelleme Formu
- Fr.0004-Rev.00-Tarafsızlık ve Gizlilik Beyanı

HAZIRLAYAN  
BGYS SORUMLUSU

ONAYLAYAN  
BİLGİ İŞLEM DAİRE BAŞKANI