

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	TAŞINABİLİR CİHAZ KULLANIMI, TAŞINABİLİR ORTAM YÖNETİMİ VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BGYS-PL02
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	23.10.2025
		Revizyon No	03
		Sayfa No	1 / 5

1. AMAÇ

Bu politikanın amacı, Gençlik ve Spor Bakanlığı personelinin uzaktan çalışma, mobil-taşınabilir cihaz ve ortamların kullanımı ile ortaya çıkabilecek risklerin yönetilerek güvenlik önlemlerinin belirlenmesini sağlamaktır.

2. KAPSAM

Bilgi Güvenliği kapsamında çalışmalar yürütülen tüm birimleri kapsamaktadır. Uzaktan çalışma, taşınabilir cihaz ve ortamların kullanımı kurum bilgileri açısından önemli riskler barındırdığından dikkatli olunması esastır.

3. UYGULAMA

3.1. Taşınabilir Cihazların Kullanımı

Bakanlığın iş süreçlerinde taşınabilir cihaz kullanılması durumunda veya kişisel taşınabilir cihazlarda Bakanlık verilerinin işlenmesi durumunda aşağıdaki kurallara uyulması gerekir.

- Bakanlık içerisinde bilgi güvenliği ile ilgili geçerli olan politika ve talimatlar, dışarıda kullanım durumunda da geçerlidir.
- Dizüstü bilgisayarlar fiziksel etkilerden korunma amacıyla kendi çantalarında taşınmalıdır. Üzerine ağır yük ve zarar verici nesneler konulmamalıdır.
- Yüksek bilgi derecesine sahip bilgilerin taşınabilir cihazlarla Bakanlık dışına çıkartılması durumunda gerekli tedbirlerin alındığından emin olunmalıdır.
- Taşınabilir cihazlar; araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karşı fiziksel olarak da korunmalıdır. Dışarıdan görünür olarak araç içerisinde taşınmamalıdır.
- Taşınabilir cihazların halka açık ağlarda kullanılmamasına özen gösterilmeli, mümkünse hotspot uygulamaları kullanılmalıdır.
- Taşınabilir cihazlar, halka açık şarj istasyonlarında şarj edilmemelidir. Çalınma, kaybolma ve yetkisiz erişim risklerine karşı taşınabilir cihazlar üzerindeki veri depolama ortamlarına şifreleme metotları uygulanmalı, ekran erişimi şifreli olmalıdır.
- Cihaz üzerindeki güvenlik uygulamaları pasif hale getirilmemeli bir hata ya da uyarı ile karşılaşıldığında sistem yöneticisi ile irtibata geçilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	TAŞINABİLİR CİHAZ KULLANIMI, TAŞINABİLİR ORTAM YÖNETİMİ VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BGYS-PL02
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	23.10.2025
		Revizyon No	03
		Sayfa No	2 / 5

- Teslim edilen dizüstü bilgisayarlar, telefon ve diğer mobil cihazlar iş amaçlı olup, kişisel amaçlı kullanılmamalıdır. Kişisel veri barındırılmamalıdır.
- Kullanılan taşınabilir cihazların yüklü yazılım sürümleri güncel tutulmalı, yüklenmesi gereken yamaların zamanında yüklenmesini sağlayacak izleme kontrolleri sağlanmalıdır.
- Çalışılacak ortamın ve çevresinin fiziksel güvenliği dikkate alınmalıdır. Gerekli durumlarda çalışılabilecek ortamlar sınırlandırılmalıdır.
- Ortak alanlarda cihaz kullanılırken ekran konumuna dikkat edilmeli 3. Taraflar tarafından ekranın görülmemesi sağlanmalıdır.
- Sesli veya görüntülü konuşma yapılması gerektiğinde sesin dışarıdan duyulmasını engellemek için uygun alanlar seçilmeli ve mümkünse kulaklık kullanılmalıdır.
- Cihazın kaybolması veya çalınması durumunda sistem yöneticisine derhal bilgi verilmeli ve gerekli önlemlerin alınması sağlanmalıdır.
- Önemli, hassas ya da kritik iş bilgilerini taşıyan cihazlar sahipsiz bırakılmamalı, mümkünse fiziksel olarak kilitlenmeli ya da cihazı güvenli hale getirmek için özel kilitler kullanılmalıdır.
- Taşınabilir cihaz kullanan personeller için, bu şekilde çalışmalardan kaynaklanan riskler ve uygulanması gereken kontroller ile ilgili olarak farkındalıklarının arttırılması amacıyla eğitim düzenlenmelidir.
- Kaynağı belli olmayan ve üretici firma tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını taşınabilir cihazlarda kullanılmamalıdır.

3.2. Taşınabilir Ortam Yönetimi

CD, DVD, USB Disk, USB Bellek, harici diskler, vb. aygıtlar, mobil cihazların depolama alanları taşınabilir ortam olarak tanımlanır. Taşınabilir ortamların yönetiminde aşağıdaki hususlara dikkat edilmelidir.

- Kaybolma, kolayca çoğaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	TAŞINABİLİR CİHAZ KULLANIMI, TAŞINABİLİR ORTAM YÖNETİMİ VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BGYS-PL02
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	23.10.2025
		Revizyon No	03
		Sayfa No	3 / 5

- Kuruma ait veriler, kişilere ait medyalar üzerinde saklanmamalı, verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılmalıdır.
- Kuruma ait medyalar varlık envanteri içinde listelenmeli ve kimler tarafından kullanıldığı kayıt altına alınmalıdır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenmeli veya ne şekilde sarf edildiği bilgisi sorgulanmalıdır.
- Çok gizli, gizli, özel ve hizmete özel veriler, taşınabilir ortamda saklanmamalıdır.
- Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/ kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmelidir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilmelidir.
- Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanmalıdır.
- Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanmalıdır.
- Taşınabilir ortamların bir yerden başka yere taşınması esnasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı gerekli önlemler alınmalıdır.
- Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen bilgi sistem cihazları ile ilgili kayıt silme işlemleri Taşınır Mal Yönetmeliğinde belirtilen usul ve esaslar çerçevesince, ilgili birimler ve komisyonlar tarafında yapılmalıdır.
- Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilmeli veya güvenli silme işlemi yapılmalıdır.
- Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	TAŞINABİLİR CİHAZ KULLANIMI, TAŞINABİLİR ORTAM YÖNETİMİ VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BGYS-PL02
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	23.10.2025
		Revizyon No	03
		Sayfa No	4 / 5

- Bilgisayarların sabit diskleri dışında hassas veri bulundurma ihtimali olan diğer depolama ortamları, ortam türüne bağlı uygun yöntem kullanılarak yok edilmelidir.

3.3. Uzaktan Çalışma

Uzaktan çalışma, alışageldiğimiz ofis çalışma ortamının dışında yapılan işin her türlüünü ifade eder. Uzaktan çalışma esnasında aşağıdaki hususlara dikkat edilmelidir.

- Uzaktan erişim için doğrudan uzak masaüstü veya terminal server gibi bağlantılar yerine SSL VPN gibi güvenli haberleşme yöntemleri kullanılmalıdır.
- Uzak masaüstü bağlantısı yapmak isteyen personel birim amirini bilgiye ekleyerek ays@gsb.gov.tr adresine mail göndermelidir. Firma görevlisi ise VPN Talep Formunu doldurup Başkanlığımıza iletmelidir.
- Çalışanın ev veya ortak internet erişimi kullanmasından doğabilecek risklerin değerlendirilmelidir. Bu bağlamda kullanıcı eğer SSL VPN ile Bakanlık kaynaklarına erişmiyorsa, internet erişimi için VPN tünelleme çözümleri değerlendirilmelidir.
- Anti virüs ve güvenlik duvarı kontrollerinin kullanıcı tarafından devre dışı bırakılmasının engellenmesi ve ilgili kontrollerin güncelliğinin sağlanması gerekmektedir.
- İşletim sistemi ve diğer yazılım ürünlerinin güncelleştirmelerinin düzenli sağlanması gerekir.
- Taşınabilir cihazların çalınma veya kaybolma riskine karşı üzerinde bulundan disklerden veri çıkmaması adına disk şifreleme yöntemleri kullanılmalıdır.
- Taşınabilir cihazlar üzerindeki verinin yedeklenmesine ilişkin gerekli kontroller sağlanmalıdır.
- Cihazların bir envanter kaydının tutularak zimmet yönetimi sağlanmalıdır.
- Uzaktan çalışmanın sona ermesi durumunda yetki ve erişim hakları iptal edilerek donanım geri alınmalıdır.
- Cihazların çalınması ya da kaybolması durumunda cihaz üzerindeki hesapların pasif hale getirilmesi ve mümkünse sıfırlanması sağlanmalıdır.

4. İlgili Dokümanlar

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	TAŞINABİLİR CİHAZ KULLANIMI, TAŞINABİLİR ORTAM YÖNETİMİ VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BGYS-PL02
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	23.10.2025
		Revizyon No	03
		Sayfa No	5 / 5

- BGYS-FRM26 VPN TALEP FORMU

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi