

1. AMAÇ

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı kapsamındaki Üniversite faaliyetlerinde kullanılan veya üniversite verilerinin işlendiği mobil cihazların kullanılması sürecinde bilgi güvenliğinin ele alınması.

2. KAPSAM:

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığındaki faaliyetlerinde kullanılan veya üniversite verilerinin işlendiği mobil cihazların kullanılması sürecinde bilgi güvenliğini kapsar.

3. YASAL DAYANAK: -

4. SORUMLULAR:

Bu talimatın uygulanmasından Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı çalışanları sorumludur.

5. UYGULAMA

Tanımlama

Mobil Cihaz	Bilgi işlenebilen taşınabilir cihazlar. Dizüstü Bilgisayar, Tablet vb.
--------------------	--

Mobil Cihaz Kullanım Kuralları

Üniversitenin iş süreçlerinde mobil cihaz kullanılması durumunda veya kişisel mobil cihazlarda üniversite verilerinin işlenmesi durumunda aşağıdaki kurallara uyulması gerekir.

- Üniversitemiz 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 veya zarar verici nesneler konulmamalıdır.
- Yüksek bilgi derecesine sahip bilgilerin mobil cihazlarla üniversite dışına çıkartılması durumunda gerekli tedbirlerin alındığından emin olunmalıdır.
- Dizüstü bilgisayarlar çalınma riskine karşı otomobil bagajında taşınmalı, dışarıdan görünür olarak araç içerisinde taşınmamalıdır.
- Mobil cihazların halka açık ağlarda kullanılmamasına özen gösterilmeli, mümkünse hotspot uygulamaları kullanılmalıdır.
- Cihaz üzerindeki güvenlik uygulamaları pasif hale getirilmemeli bir hata ya da uyarı ile karşılaşıldığında sistem yöneticisi ile irtibata geçilmelidir.
- Teslim edilen dizüstü bilgisayarlar, telefon ve diğer mobil cihazlar iş amaçlı olup, kişisel amaçlı kullanılmamalıdır. Kişisel veri barındırılmamalıdır.
- Kullanılan mobil cihazların yüklü yazılım sürümleri güncel tutulmalı, yüklenmesi gereken yamaların zamanında yüklenmesini sağlayacak izleme kontrolleri sağlanmalıdır.
- Çalınma, kaybolma ve yetkisiz erişim risklerine karşı mobil cihazlar üzerindeki veri depolama ortamlarına şifreleme metotları uygulanmalı, ekran erişimi şifreli olmalıdır.
- 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.

Uzaktan Çalışma Güvenlik Kontrolleri

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.
- Çalışanın ev veya ortak internet erişimi kullanmasından doğabilecek risklerin değerlendirilmesi. Bu bağlamda kullanıcı eğer SSL VPN ile üniversite kaynaklarına erişmiyorsa, İnternet 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 sağlanmalı.
- Cihazların bir envanter kaydının tutularak zimmet yönetimi sağlanmalı.
- 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.