1. AMAÇ

Bu prosedürün amacı, bilgi içeren taşınabilir cihazların kullanımı sırasında göz önüne alınması gereken güvenlik konularını tanımlamaktır.

2. KAPSAM

Bu prosedür, Üniversite tarafından kişiye tahsis edilen taşınabilir cihazları kullanan tüm kullanıcıları / KU mensuplarını ve mezunları kapsamaktadır.

3. REFERANSLAR

3.1. KU Bilgi Teknolojileri Yönetişim Yönergesi

3.2. KU Bilgi Güvenliği Yönergesi

3.3. KU Kurumsal Hat Kullanımı ve Cep Telefonu Prosedürü

3.4. KU Kişisel Bilgisayar Tahsis ve İşletim Prosedürü

3.5. YÖK Öğrenci Disiplin Yönetmeliği

3.6. Koç Üniversitesi İdari Personel Yönetmeliği

3.7. COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetişim bileşenlerinin ilgili yönetişim ve yönetim hedefine uygulanabilecek her biri.

3.8. ISO 27000:2013 Bilgi Güvenliği yönetim standartları ailesi tamamı.

3.9. SANS-CIS kontrolleri: En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.

3.10. 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.11. 6698: Kişisel Verilerin Korunması Kanunu

3.12. 4857: İş Kanunu

3.13. 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1. Bu prosedürün uygulatılmasından Bilgi Güvenliği Komitesi sorumludur.

4.2. Bu prosedürün hazırlanmasından ve güncellenmesinden Bilgi Teknolojileri Direktörlüğü sorumludur

4.3. Bu prosedürün, devreye alınmasından, iyileştirme takibinin yapılmasından ve taşınabilir cihaz kullanımı standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

5. TANIMLAR

5.1. **KU mensupları:** İdari çalışanlar, akademik çalışanlar, öğrenciler

5.2. **Bilgi Sistemleri:** Bilgi sistemleri, Üniversite'nin sahip olduğu, kiraladığı, uyarladığı, muhafaza altına aldığı veya kontrolü altında olan kaynakları; bu kapsamda kişisel veya kurum tarafından sağlanan bilgisayarları, ağları, bulut ve internet temelli hizmetleri, taşınabilir cihaz/depolama aygıtlarını, yazılımları ve bunlar ile ilgili her türlü donanım, teçhizat ve fikri mülkiyeti ifade eder.

5.3. **MDM:** Mobile Devices Management – Mobil Cihaz Yönetimi

5.4. **Taşınabilir Cihaz:** Üniversiteye ait tüm ağlara, verilere ve sistemlerine erişimi olan akıllı telefon, tablet ve laptop vb. cihazlar.

6. TEMEL PRENSİPLER

6.1. Bu prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU idari personeli için 4857 sayılı İş Kanunu ve Koç Üniversitesi İdari Personel Yönetmeliği, KU akademik personel için 2547 sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilir.

6.2. Bilgi İçeren Taşınabilir Cihazların Fiziksel Güvenliği için Uygulanacak Kurallar

6.2.1. Üniversite tarafından personelin üzerine zimmetlenen bilgi içeren taşınabilir cihazların fiziksel güvenliğine azami dikkat gösterilmelidir. Örnek olarak: Yolculuk (otobüs, tren, uçak, v.b.) sırasında bilgisayarlar, bagaj olarak değil el çantası olarak taşınır, dışarıdan görünür şekilde araç içinde bırakılmaz.

6.2.2. Cihazların bozulması durumunda eski cihaz onarımı süresince mümkün olması halinde geçici cihaz personele teslim edilir. Belirli periyotlarda cihazlar yenilenmektedir.

6.2.3. Yeni cihazların teknoloji değerlendirmeleri Bilgi Teknolojileri Direktörlüğü tarafından yapılır.

6.2.4. Bilgi Teknolojileri Direktörlüğü tarafından sağlanan bilgi içeren taşınabilir cihazlar Bilgi Teknolojileri Direktörlüğü tarafından zimmet kaydı alınır ve takip edilir.

6.2.5. Üniversite tarafından sağlanan taşınabilir cihazların çalınması/kaybolması durumunda Bilgi Güvenliği birimi ile iletişime geçilmeli, Kişisel Bilgisayar Tahsis ve İşletim Prosedürü ve Kurumsal Hat Kullanımı ve Cep Telefonu Prosedürü işletilmelidir.

6.3. Bilgi İçeren Taşınabilir Cihazlarda Bulunan Verilerin Korunması için Uygulanacak Kurallar

6.3.1. Bilgi içeren taşınabilir cihazlardaki kurumsal veriler Üniversite tarafından sağlanan ortak alanlarda saklanır.

6.3.2. Üniversite standartlarına uygun olarak onaylanmış şifreleme yöntemleri ve yazılımları kullanılmaktadır.

6.3.2.1. Bütün taşınabilir bilgisayarların sabit disklerinde şifreleme uygulanır. Üniversite akademik araştırmalar ile özel amaçla alınmış (proje özelinde) taşınabilir cihazlar bu şifreleme süreçlerine dahil değildir.

6.3.3. Üniversite tarafından sağlanan tüm mobil cihazlarda Mobil Cihaz Yönetimi (MDM) uygulanır.

6.3.4. Bilgisayarların ekran koruyucuları devrede ve parola korumalı olmalıdır.

6.3.5. Kullanıcı tarafından iade edilen içerisine veri depolanan taşınabilir cihazlar içlerindeki veriler geri dönüşümsüz şekilde silinerek yeniden kullanım için hazırlanır.

6.3.6. Mobil cihazlarda hukuki açıdan suç teşkil edecek belgeler (resmi makamlardan gelmiş gizli bilgi şeklinde etiketlenmiş dokümanlar, bilgisayar ve ağ güvenliğini yok edebilen, zarar verebilen belge, yazılım ve materyal) bulundurulmamalıdır.

6.3.7. Cihazlara kurulan kişisel elektronik posta ve diğer kişisel iletişim uygulamaları kullanılırken tanınmayan kişi ya da kaynaktan gelen mesaj ve dosyalara dikkat edilmelidir.

6.4. Tanım dışı durumlar Bilgi Güvenliği Komitesi tarafından değerlendirilmektedir.

7. YÖNTEM

7.1. Mobil Cihaz Yönetim Kuralları

7.1.1. Akıllı telefon ve tabletler sürekli gelişen ve değişen işlevsellikleriyle diğer mobil cihazlardan farklı güvenlik tehditlerine açık durumdadırlar. Bu sebeple akıllı telefon ve tablet gibi mobil cihazları kişisel güvenlik önlemleri ile yönetmek yetersiz kalmakta, uygun güvenlik uygulamaları ile doğru kurallar uygulanmadığı takdirde veriye ve altyapıya yetkisiz erişimler kaçınılmaz olmaktadır.

7.1.2. Mobil cihazlardan Üniversite bilgi sistemlerine yapılan erişimlerde veri ve sistem güvenliği sürekliliğinin sağlanması Mobil Cihaz Yönetim sistemi (Mobile Device Management) aracılığıyla sağlanır.

7.1.3. Üniversite'nin sistemlerine erişim yetkisi olan mobil cihazlara MDM uygulaması yüklenir ve tüm cihazlar yönetim ara yüzünde kayıt altına alınır.

7.1.4. Mobil Cihaz Yönetim sisteminin işletim araçları bu dokümanda belirtilen bilgiler dışında cihazlarda yer alan hiç bir içeriğe (elektronik posta/mesajlaşma içerikleri, arama kaydı vb.) erişime olanak tanımamaktadır. Kişisel bilgileri sistemi işletmekle sorumlu ekiplerin dahi takip etmesi, izlemesi ya da kayıt altına alması bu nedenle mümkün değildir.

7.2. Mobil Cihaz Güvenliği Kuralları

7.2.1. iOS ve Android işletim sistemlerine sahip mobil cihazlara Üniversite ağlarına erişim yetkisi verilebilir.

7.2.2. MDM sistemi prosedür kapsamındaki cihazların marka ve modelini, IMEI numarasını, seri numarasını, wireless-mac ID bilgilerini kayıt altına alır.

7.2.3. E-posta kurulumu için cihazlarda 2 farklı platform (Exchange Online ve G Suite) seçeneği bulunmaktadır. Cihazlarında Exchange Online kullanan idari-akademik personel kişisel cihazına e-posta kurmak istediğinde sistem "Android Administrator" uygulaması olarak cihaza yerleşmektedir, ancak Gmail (G Suite) kullanan cihazlar için bu sıkılaştırma uygulanamamaktadır.

7.3. Mobil Cihaz Yönetim Sistemi ile Cihaz Güvenliği

7.3.1. Prosedür kapsamındaki mobil cihazlara yetkisiz erişimi önlemek için ekran parolası zorunlu olarak uygulanır.

7.3.2. Yazılım Geliştirme ve BT Operasyon Birimi, MDM uygulaması ile sanal özel ağ (VPN) ve Wi-Fi yapılandırmalarını uzaktan otomatik olarak gerçekleştirir.

7.3.3. Personelin iş gereksinimleri sebebiyle erişime yetkili olduğu programlar, mobil cihazlarda yer alan yönetilen uygulama marketi aracılığıyla kullanıcı tarafından yüklenir.

7.3.4. Mobil cihazların yama ve güncelleme konfigürasyonları otomatik olarak yüklenecek şekilde gerçekleştirilir. Bu konfigürasyonlar Yazılım Geliştirme ve BT Operasyon Birimi tarafından takip edilir.

7.3.5. Üniversite tarafından sağlanan tüm kurumsal mobil cihazlar MDM'e dahil edilir.

7.3.6. Mobil cihazlarda cihaz bütünlüğünü bozarak cihazın güvenlik özelliklerini yitirmesine sebep olan; cihaz sistemini kırma (jailbreak), kök dizini değiştirme (root) işlemi yapılmış cihazlardan elektronik posta ve Üniversite ağına erişim yapılması engellenir.

7.3.7. Kötü amaçlı yazılım ya da zararlı uygulama olduğu tespit ve teyit edilmiş yazılım ve uygulamaların kullanımı durdurulur.

7.3.8. MDM uygulamasının mobil cihaz konum tespit özelliği, MDM uygulaması yüklü olan ve sadece kayıp ya da çalıntı iOS cihazlar için etkinleştirilebilir.

7.3.9. Cihaz içindeki verilere yetkisiz erişimleri engellemek için kayıp ya da çalıntı cihazlar mümkün olan en kısa zamanda BT Servis masasına bildirilerek verilerin uzaktan silinmesi sağlanmalıdır. Personelin işten ayrılması durumunda da cihaz içeriği uzaktan silinebilir. (Kullanıcıların mobil cihazlarındaki kişisel verilerini yedeklemeleri kendi sorumluluklarındadır).

7.3.10. Bağlantı ve işletim sistemi ile ilgili sorunlarda BT Servis Masası ile irtibata geçilmelidir.

7.3.11. Mobil cihazlara uygulama yüklenirken, yüklenen uygulamaların güvenliğinden emin olunmalı ve uygulamayı yazan üretici firmanın tanınırlığına (Android cihazlarda play protect damgası) dikkat edilmelidir.

7.4. MDM İşletimi

7.4.1. Profiller

Android cihazları 4 farklı profile sahiptir.

7.4.1.1. Android Cihazlarda Kaydolma Profilleri

1. Corporate-owned fully managed user devices (Fully Managed)
2. Corporate-owned devices with work profile (Work Profile)
3. Personal and corporate-owned devices with administrator privileges (Device Administrator)
4. Corporate-owned dedicated devices (Kiosk - Task Devices)

7.4.1.2. "Fully Managed" Profili Kayıt Aşamaları

Cihaz ilk açılışta veya fabrika ayarlarına döndürüldüğünde aşağıdaki aşamalar uygulanır.

1. Silinmiş/Yeni cihazınızı açın.
2. Hoş Geldiniz ekranında dili seçin.
3. Wi-Fi ağınıza bağlanın ve İLERİ'yi seçin.
4. Google hüküm ve koşullarını kabul edin ve ardından İLERİ'yi seçin.
5. Google oturum açma ekranında bir Gmail hesabı yerine afw#setup girin ve İLERİ'yi seçin.
6. Android Cihaz İlkesi uygulaması için YÜKLE'yi seçin.
7. Bu ilkenin yüklemesine devam edin. Bazı cihazlar ek koşulların kabul edilmesini gerektirebilir.
8. Bu cihazı kaydet ekranında cihazınızın QR kodunu taramasına izin verin veya belirteci el ile girmeyi seçin.
9. Kaydı tamamlamak için ekrandaki istemleri takip edin.
10. Intune'da gösterilen QR kodu taratın veya kodu elle girin.
11. Kurum e-posta adresi ve parolasını girin.

7.4.1.3. "Work Profile" Profili Kayıt Aşamaları

Cihaz ilk açılışta veya fabrika ayarlarına döndürüldüğünde olası kurulum ekrandaki yönergeler ile tamamlanır.

1. Microsoft Intune uygulaması Play Store'dan yüklenir.
2. Intune aracılığıyla "work profile" kurulumu tamamlanır.
3. Ön tanımlı uygulamalar otomatik olarak yüklenir.

7.4.1.4. "Device Administrator" Profili Kayıt Aşamaları

Cihaz ilk açılışta veya fabrika ayarlarına döndürüldüğünde olası kurulum ekrandaki yönergeler ile tamamlanır.

1. Microsoft Intune uygulaması Play Store'dan yüklenir.
2. Microsoft Intune cihaz yönetimi yetkilisi olarak ayarlanır.

7.4.1.5. "Kiosk - Task Devices" Profili Kayıt Aşamaları

Cihaz ilk açılışta veya fabrika ayarlarına döndürüldüğünde aşağıdaki aşamalar uygulanır.

1. Silinmiş/Yeni cihazınızı açın.

2. Hoş Geldiniz ekranında dili seçin.
3. Wi-Fi ağınıza bağlanın ve İLERİ'yi seçin.
4. Google hüküm ve koşullarını kabul edin ve ardından İLERİ'yi seçin.
5. Google oturum açma ekranında bir Gmail hesabı yerine afw#setup girin ve İLERİ'yi seçin.
6. Android Cihaz İlkesi uygulaması için YÜKLE'yi seçin.
7. Bu ilkenin yüklemesine devam edin. Bazı cihazlar ek koşulların kabul edilmesini gerektirebilir.
8. Bu cihazı kaydet ekranında cihazınızın QR kodunu taramasına izin verin veya belirteci el ile girmeyi seçin.
9. Kaydı tamamlamak için ekrandaki istemleri takip edin.
10. Intune'da gösterilen QR kodu taratın veya kodu elle girin.

7.4.2. MDM Yüklü Cihazlarda İzin Yönetimi

MDM yüklü cihazlarda aşağıda yer alan profillere göre yapılabilen müdahaleler yer almaktadır.

7.4.2.1. "Fully Managed" Cihazlarda

1. Wipe
2. Delete device
3. Remote lock
4. Reset Passcode
5. Restart

7.4.2.2. "Work Profile" Cihazlarda

1. Retire
2. Delete device
3. Remote lock
4. Force sync
5. Reset Passcode
6. Send Custom Notification
7. Remote assistance (TeamViewer lisansı gerekir.)

7.4.2.3. "Device Administrator" Cihazlarda

1. Retire

2. Wipe
3. Delete device
4. Remote lock
5. Force sync
6. Send Custom Notification
7. Remote assistance (TeamViewer lisansı gerekir.)

7.4.2.4. "Kiosk – Task" Cihazlarda

1. Wipe
2. Delete device
3. Remote lock
4. Reset Passcode
5. Restart

Bu listedekiler dışında (konum bulma, SMS okuma, ekran görüntüsü alma, ayar değiştirme) bir işlem yapılamamaktadır.

7.4.3. MDM Yüklü Olmayan Cihazlarda İzin Yönetimi

MDM olmayan cihazlarda;

1. Conditional access policy uygulanabilir.
2. Exchange Online Outlook için cihazda "Device Manage" tanım zorunluluğu bulunmaktadır.

8. EKLER VE KAYITLAR

Yoktur.

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü'ne aittir. Gözden geçirme sürekli olarak yapılır. Gerekli görüldüğü zaman ve durumlarda prosedürün revize edilmesi gereklidir.

10. DEĞİŞİKLİK/ DAĞITIM/ ONAY TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			