T.C.
İSTANBUL
KÜLTÜR
ÜNİVERSİTESİ

İKÜ BST

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

MOBİL CİHAZ VE TAŞINABİLİR ORTAM KULLANIM POLİTİKASI (MCTOKP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme	İsmail Koç	
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Rektörlük Temsilcisi

İÇİNDEKİLER

1. AMAÇ

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde çalışan personelin kullanmış olduğu depolama cihazlarında bulunan bilgilere yetkisiz kişilerin erişimini engellemek için asgari gereksinimleri tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde kullanılan CD/DVD, harici bellek, taşınabilir disk sürücü türevi cihazlar, tablet, Cep telefonu ve notebook gibi bilgi işleme ve saklama kapasitesine sahip tüm taşınabilir cihazların kullanımını kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.6.2.1 maddesi.
- 15.03.2018 tarihli ve 19924119-719-E.21240 sayılı "2016-2019 Ulusal Siber Güvenlik Eylem Planı" konulu YÖK yazısında, üniversitelerin ISO27001 Bilgi Güvenliği Yönetim Sertifikası alması ve iş süreçlerini bu şekilde yapılandırması gerektiği ifade edilmiştir.

4. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
BGYS	Bilgi Güvenliği Yönetim Sistemi
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
İKÜ	T.C. İstanbul Kültür Üniversitesi
KVKK	6698 Numaralı Kişisel Verilerin Korunumu Kanunu
WEB	Wireless Equivalent Privacy: 802.11 standardındaki kablosuz ağlarda kullanılan bir şifreleme yöntemidir.

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
2	IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü
3	Duran Varlık Ürün Kullanıcısı Bilgi Formu
4	Teslim Tutanağı

5	IKU BSTDB Sigorta Prosedürü

6. MOBİL CİHAZ KULLANIM VE TAŞINABİLİR ORTAM POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

6.1. İKÜ ayniyatına dahil olan tüm mobil cihazlar (cep telefonu, dizüstü bilgisayar, tablet, harici bellek, taşınabilir disk sürücü vb.) ilgili kişiye Ayniyat Birimi tarafından zimmetlenerek, BSTDB Destek Birimi tarafından "Duran Varlık Ürün Kullanıcısı Bilgi Formu" ve "Teslim Tutanağı" ile teslim edilir.

6.2. Tüm İKÜ personeli kendisine zimmetlenen cihaz/cihazların güvenliğinden ve amacına uygun kullanımından sorumludur.

6.3. Mobil cihaz, çalınma ya da kaybolma riskini azaltmak için, seyahat sırasında, konferans merkezleri ve toplantı salonları gibi yerlerde, araba ve diğer ulaşım araçlarında, otel odalarında, kalabalık ortamlarda ve güvensiz halka açık ortamlarda başıboş bırakılamaz.

6.4. İKÜ personelinin, İKÜ tarafından kurumsal amaçla verilen mobil cihazların kendisi dışında herhangi bir kimseye (aile fertleri, iş yeri çalışanları vb.) kullandırması ve paylaşması yasaktır.

6.5. İKÜ personeli, mobil cihazlarda saklanan bilgilerin gizlilik seviyesinin farkında olmalı ve İKÜ 'ye ait, gizlilik içeren, kritik, hassas ve KVKK kapsamındaki bilgiler mümkün olduğunca mobil cihazlar üzerinde bulundurulmamalıdır.

6.6. İçerisinde İKÜ 'ye ait bilgilerin olduğu mobil cihazlara yetkisiz müdahaleyi önlemek amacıyla cihazı kullanan tarafından şifre tanımlanması zorunludur.

6.7. İKÜ tarafından belirlenen "Gizli" gizlilik seviyesindeki kurum bilgilerini içeren taşınabilir depolama cihazı, üst yönetimin onayı olmadıkça İKÜ dışına çıkarılamaz.

6.8. İKÜ tarafından belirlenen "Hizmete özel" gizlilik seviyesindeki kurum bilgilerini içeren taşınabilir depolama cihazı, sadece laptop gibi parola koruması olan ortamlarla İKÜ dışına çıkarılabilir.

6.9. Bilginin İKÜ dışına çıkarılma durumlarında, aygıtların korunmasından dışarıya çıkarma işlemini gerçekleştiren İKÜ personeli sorumludur.

6.10. İKÜ içerisinde "Hizmete özel" veya daha üst seviye gizlilik seviyesinde gizli bilgi bulunan depolama aygıtları parola korumasız olarak ortamlarda başıboş bırakılamaz.

6.11. İKÜ içerisindeki taşınabilir ortamda bilginin sorumluluğu da bilgiyi son teslim alan (yedekleyen, işleyen vs.) İKÜ personelindedir.

6.12. Mobil cihazlar bilgisayar ya da sistemlerde kullanılmadan önce mutlaka İKÜ bünyesinde kullanılan güncel anti-virüs yazılımının taramasından geçirilmek zorundadır.

6.13. İKÜ bünyesinde "Gizlilik", "bütünlük" veya "erişilebilirlik" seviyesi "yüksek" olarak tanımlanmış ya da daha üst seviyede olan bilgisayar ve sistemlere, güvenliği sistemli ve sürekli olarak kontrol edilen cihazlar dışında taşınabilir depolama cihazı takılamaz.

6.14. Depolama cihazlarındaki bilgilere olan ihtiyaç sona erdiğinde, aygıt içerisindeki bilgiler cihaz sorumlusu tarafından "IKU BSTDB Ortamın Güvenli Yok Edilme Prosedürü" ne göre silinmelidir.

6.15. CD/DVD gibi silinemeyen aygıtlar eğer "gizli" seviyesinde bilgi içeriyorsa kırpma makinesi ile imha edilmelidir. Daha düşük seviyeli kurum bilgilerini içeren ortamlar fiziksel olarak kırılma, parçalanma gibi yöntemlerle imha edilmelidir.

6.16. CD ve DVD gibi optik ortamlarda veri barındırırken kaliteli ortamlar tercih edilir, ortamların önerilen fiziksel ve çevresel koşullarına uyulur.

6.17. Mobil cihazlara, İKÜ 'nün izin verdiği yazılımlar dışında yazılım kurulamaz.

6.18. Mobil cihazlardaki bilgilerin "gizli, bütün ve erişilebilir" kalabilmesi için bu bilgilerin asıl kopyaları İKÜ sunucularında barındırılırlar.

6.19. Mobil cihaz kullanıcıları mobil cihaza yeni bileşen ekleyemez, çıkartamaz ya da mevcut bileşenlerin ayarını değiştiremez. Bu işlemleri gerçekleştirebilecek tek yetkili BSTDB Destek Birimidir.

6.20. Taşınabilir veri depolama ortamları, veri yedekleme amacıyla kullanılmaz.

6.21. Kaynağı güvenilir olmayan yerlerden temin edilen taşınabilir veri depolama ortamları kullanılmaz.

6.22. İKÜ 'ye ait gizli bilgiler, bilginin açık olarak paylaşıldığı bulut servislerinde işlenemez ve barındırılamaz.

6.23. Mobil cihaz yazılım sürümleri ve yamaların uygulanması için mobil cihaz yönetim yazılımı kullanılır.

6.24. İKÜ isterse mobil cihazları uzaktan devre dışı bırakabilir, silme ya da kilitleme işlemleri gerçekleştirebilir.

6.25. Güvenli protokollere sahip olmayan (http://) Web hizmetlerinin ve web uygulamalarının kullanımı ve sorumluluğu mobil cihaz kullanıcısına aittir.

6.26. Mobil cihaz kullanıcısı, mobil cihazlar ile güvenilir olmayan kablosuz ağlara (WEP, Ortak ağlar) bağlanmamalıdır.

6.27. Mobil cihazların çalınması ya da kaybolması durumları için yasal, sigorta ve kuruluşun diğer güvenlik gereksinimleri dikkate alınarak "IKU BSTDB Sigorta Prosedürü" dokümanı işletilir.

6.28. İKÜ personelinin kendisine ait mobil cihazını kullanması durumunda;

6.28.1. Cihazların özel ve iş kullanımının ayrılması gerekmektedir. Bunun için kişisel mobil cihazına mobil cihaz yönetim yazılımının kurulması gerekmektedir.

6.28.2. Kullanıcıların görevlerini kabul ettikleri "IKU BSTDB Personel Gizlilik Sözleşmesi" imzalamalarından sonra iş bilgilerine erişim sağlanması (fiziksel koruma, yazılım güncelleme vb.), iş verilerinin sahipliğinden feragat, cihazın çalınması ya da kaybolması ya da hizmetin kullanımı yetkilendirmesi için vakit olmadığında kuruluş tarafından verilerin uzaktan silinmesine izin verilir.

6.28.3. İKÜ tarafından mobil cihaz üzerindeki kişisel veriler cihaz sahibinin rızası olmadan görüntülenmez, kopyalanmaz, taşınmaz ya da silinmez.

7. MOBİL CİHAZ VE TAŞINABİLİR ORTAM KULLANIM POLİTİKASININ YAPTIRIMLARI

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla "IKU BSTDB Bilgi Güvenliği Disiplin Politikası" ve "IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü" belgelerinde belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

8. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar