İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

TEMİZ MASA TEMİZ EKRAN POLİTİKASI (TMTEP)

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 bünyesindeki kâğıtlar, taşınabilir depolama ortamları ve kişisel bilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak amacıyla gerekli olan şartları tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde çalışan tüm personeli kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.11.2.9 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: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, sözleşmeleri, talimatları, prosedürleri, prosesleri ve tüm kaynakları içerir.
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
E-POSTA	Elektronik Posta
İKÜ	T.C. İstanbul Kültür Üniversitesi
POST-IT	Yapışkan Kâğıt

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	İKÜ BSTDB Parola Yönetimi Politikası
2	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
3	IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü

4	IKU BSTDB Ortamın Güvenli Yok Edilme Prosedürü
5	IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası

6. TEMİZ MASA TEMİZ EKRAN POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

6.1. Kuruma ait uygulamalarda kullanılan parolalar iş arkadaşları da dâhil olmak üzere kimse ile paylaşılamaz, parolalar yazılı olarak post-it ya da not kâğıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılamaz.

6.2. Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapıları kilitli tutulur.

6.3. Evrak ve dokümanlardaki bilgiler, farklı kişilerin eline geçmemesi için klasörlerde saklanır.

6.4. Hassas bilgi içeren evrak klasörleri ve kuruma ait başlıklı kâğıtlar kilitli dolaplarda saklanır.

6.5. Kâğıtlar çöp kutularına atılmak yerine, kâğıt imha makinalarında kırpılır.

6.6. Hassas ve kritik bilgi içeren evraklar ağ üzerinden paylaşılamaz.

6.7. Masa üstü doküman sayısını artırmamak adına mümkün olduğu kadar elektronik dokümanın yazıcıdan çıktılarının alınmamasına dikkat edilir.

6.8. Masa üzerinde, kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılmaz ve bunlar kilitli çekmecelerde muhafaza edilir.

6.9. Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.

6.10. İKÜ 'ye ait kritik bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.

6.11. Personelin kişisel gizli bilgileri (maaş bordrosu vb.) başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.

6.12. Personel telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmalıdır.

6.13. Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilir.

6.14. İKÜ bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanlar toplantı sonrasında ilgili salonlarda bırakılamaz ve salonlardaki tahtalara alınmış notlar silinir.

6.15. Gizlilik içeren bilgiler umumi yerlerde konuşulamaz.

6.16. Gizlilik içeren bilgiler, telefonlarda dışarıya ses açık olarak görüşülemez. Faks yoluyla gizlilik içeren herhangi bir bilgi gönderilmez.

6.17. Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekir.

6.18. Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılamaz.

6.19. Bilgisayarlar gözetimsiz bırakıldığında kapatılır veya parola kullanılarak korunur. Ekran koruyucusu aktif hale getirilmelidir.

6.20. Uygulamalarda ya da ağ hizmetlerinde yapılacak işlem tamamlandıktan sonra oturum kapatılır.

6.21. Fotokopi cihazlarının belleğinde kritik ve hassas bilgiler bulundurulamaz.

6.22. Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinir.

6.23. Parolalar yazılı olarak saklanamaz ve gizli tutulur.

6.24. Personel bilgisayarındaki, taşınabilir belleğindeki, harici diskte ve benzeri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli veya önemli veri konulması gerekiyorsa kriptolanarak korunur.

6.25. Gizli belgelerin, parolaların, adreslerin, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşılmamasına dikkat edilir.

6.26. Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.

6.27. Elektronik posta ortamında kişisel parola bilgileri paylaşılamaz.

6.28. Silinebilir ortamlara kaydedilmiş olan gizli bilgiler kullanımdan sonra "IKU BSTDB Ortamın Güvenli Yok Edilme Prosedürü" çerçevesinde geri dönülmeyecek şekilde silinir.

6.29. Kuruma ait yürütülen iş ve işlemlerde @iku.edu.tr adresi kullanılmalıdır.

6.30. Kurumsal işlerin yapıldığı bilgisayarlar personelin kendi sorumluluğundadır. Kurum bilgisayarlarını personel haricinde yetkisiz kullanıcılara teslim edilemez.

6.31. Fotokopisi alınan belgelerin orijinalleri ve kopyaları fotokopi cihazında bırakılamaz. Yazıcıdan alınan çıktılar yazıcının üstünde bırakılamaz.

6.32. Parolalara ek olarak, kimlik kartı ve e-imza cihazı gibi kişiye özel yetkilere sahip nesneler de paylaşılmaz.

6.33. Gözetimsiz cihazların kullanımı ile ilgili "Varlıkların Kabul Edilebilir Kullanımı Politikası" dokümanı içerisinde yer alan 7.bölüm maddeleri geçerlidir.

7. TEMİZ MASA TEMİZ EKRAN 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
TMTEP-001-2.0		6.33. Gözetimsiz cihazların kullanımı ile ilgili "Varlıkların Kabul Edilebilir Kullanımı Politikası" dokümanı içerisinde yer alan 7.bölüm maddeleri geçerlidir. (Yeni Madde Ekleme)	Ufuk Dikme

TMTEP-001-2.0		5. Bölüm İlgili Dokümanlar kısmına IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası eklendi.	Ufuk Dikme