

İSTANBUL KÜLTÜR ÜNİVERSİTESİ
BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE
BAŞKANLIĞI
ERİŞİM KONTROL POLİTİKASI (EKP)

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

Doküman Kod	IKU-BSTDB-EKP-001	Revizyon Tarihi	26.02.2022
Yayın Tarihi	02.10.2020	Revizyon No	EKP -001-2.0

İÇİNDEKİLER

1. AMAÇ	3
2. KAPSAM	3
3. DAYANAK.....	3
4. TANIMLAR VE KISALTMALAR	3
5. İLGİLİ DOKÜMANLAR	3
6. ERİŞİM KONTROL POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ.....	4
7. ERİŞİM KONTROL POLİTİKASININ YAPTIRIMLARI	5
8. REVİZYON BİLGİSİ	5

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

Doküman Kod	IKU-BSTDB-EKP-001	Revizyon Tarihi	26.02.2022
Yayın Tarihi	02.10.2020	Revizyon No	EKP -001-2.0

1. AMAÇ

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesindeki bilgiye erişim için kullanılacak yöntemleri tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde bulunan bilgiye erişilecek tüm kuralları kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.9.1.1 ve A.9.4.1 maddeleri.
- 5651 numaralı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
- 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
ADMINISTRATOR	Yönetici Hesabı
BGYK	Bilgi Güvenliği Yönetim Kurulu
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
EBYS	Elektronik Belge Yönetim Sistemi
İKÜ	T.C. İstanbul Kültür Üniversitesi
PAM	Privileged Access Management (Ayrıcalıklı Hesap Yönetimi), kritik varlıklara erişimi kontrol etmenize, yönetmenize ve izlemenize yardımcı olan bir çözümdür.
PDKS	Personel Devam Kontrol Sistemi
VLAN	Sanal yerel alan ağı anlamına gelen VLAN, yerel ağ içerisinde çalışma grupları oluşturmak, yerel ağ anahtarlarla bölmektir.

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
----	----------------

Doküman Kod	IKU-BSTDB-EKP-001	Revizyon Tarihi	26.02.2022
Yayın Tarihi	02.10.2020	Revizyon No	EKP -001-2.0

1	İKÜ BSTDB Ağ ve Ağlara Erişim Politikası
2	İKÜ BSTDB Şifre Yönetimi Politikası
3	İKÜ BSTDB Personel Gizlilik Sözleşmesi
4	İKÜ BSTDB Kurumsal Gizlilik Taahhünamesi
5	İKÜ BSTDB Uzaktan Erişim Politikası

6. ERİŞİM KONTROL POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

- 6.1. İKÜ bilgisayar ağına erişim, “İKÜ BSTDB Ağ ve Ağlara Erişim Politikası” ile düzenlenir.
- 6.2. İKÜ bilgisayar ağı kendi içinde VLAN teknolojisi ile birbirlerinden ayrılır.
- 6.3. Sistem üzerinde kullanıcı oluşturma işlemi “SAP Orion” yazılımı ile iş girişine müteakip otomatik olarak yapılır.
- 6.4. Sistem üzerinde kullanıcı otomatik oluşturulduktan sonra, birim bazında yetkilendirme ve roller AD ve SAP Orion uygulamaları tarafından otomatik yapılır.
- 6.5. Sistem üzerinde kullanıcı silme işlemi “SAP Orion” yazılımı ile istihdamın sonlandırılmasına müteakip otomatik olarak yapılır.
- 6.6. Ayrıcalıklı erişim hakları yalnızca sistem yöneticileri ve network yöneticilerine verilmektedir. Diğer kullanıcıların hakları kısıtlanmıştır. Sunucular üzerinde, yalnızca sistem ve network yöneticilerinin “Administrator” ayrıcalıklı erişim hakkı vardır.
- 6.7. Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi için, kimlik yönetimi yazılımı kullanılır. Her kullanıcıya İKÜ tarafından belirlenen bir kullanıcı adı ve “İKÜ BSTDB Şifre Yönetimi Politikası” dokümanına göre şifre verilir. Kullanıcılar sistemlere kendilerine ait kullanıcı adı ve şifre ile bağlanır.
- 6.8. İKÜ bünyesinde yerleşke girişlerinde personel kartı ile turnike sistemleri kullanılır.
- 6.9. İKÜ bünyesinde PDKS sistemi kullanılır.
- 6.10. İKÜ yasal mevzuat gereği EBYS kullanır. Resmi dokümanlar yetkili personeller tarafından E-imza ile imzalanır.
- 6.11. Erişim hakları İKÜ BGYK tarafından düzenlenen YGG toplantılarında gözden geçirilir ve kurulun uygun gördüğü değişiklikler BSTDB tarafından uygulanır.
- 6.12. Kullanıcılara verilen şifrelerin ifşa edilmeyeceği taahhüdü “İKÜ BSTDB Personel Gizlilik Sözleşmesi” ile alınır.
- 6.13. Hizmet alınan yüklenici tarafından yapılacak erişimler “İKÜ BSTDB Kurumsal Gizlilik Taahhünamesi” kullanılarak yapılır. Yüklenici personeli tarafından erişimler kurum tarafından oluşturulmuş kimlik doğrulama bilgisi kullanılarak sağlanır.
- 6.14. Ayrıcalıklı haklar Ağ ve İletişim ve Sistem İşletim müdürlükleri tarafından yönetilir. Yazılım kurulumu kısıtlamalarında BSTDB personeli ayrıcalıklı haklara sahip olup kendi bilgisayarlarında program kurabilir. Aynı zamanda internet erişimlerinde ayrıcalıklı haklar kullanılır.

Doküman Kod	İKÜ-BSTDB-EKP-001	Revizyon Tarihi	26.02.2022
Yayın Tarihi	02.10.2020	Revizyon No	EKP -001-2.0

- 6.15. Özel sistemlere erişim hakları aylık olarak gözden geçirilir ve gerekli hallerde özel sistemlere erişim hakları kaldırılır.
- 6.16. Yüklenicilerin erişim kontrol rolleri sadece BSTDB tarafından verilir.
- 6.17. İş uygulamalarına uzaktan erişim için “İKÜ BSTDB Uzaktan Erişim Politikası” dokümanı kullanılır.
- 6.18. “açıkça yasaklanmadıkça her şeye izin verilir” kuralının aksine “açıkça izin verilmedikçe her şey yasaklanır” kuralı geçerlidir.
- 6.19. Kullanıcılara sadece, görevlerini gerçekleştirmek için gereken bilgilere/uygulamalara erişim verilir. (Farklı görevler/roller, farklı bilmesi gereken ve farklı erişim profili demektir.)

7. ERİŞİM KONTROL POLİTİKASININ YAPTIRIMLARI

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla “İKÜ BSTDB Bilgi Güvenliği Disiplin Politikası” ve “İKÜ 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
EKP-001-2.0		6.15 Özel sistemlere erişim hakları periyodik (aylık) olarak gözden geçirilir ve gerekli hallerde özel sistemlere erişim hakları kaldırılır.	Ufuk Dikme
EKP-001-2.0		6.19. Kullanıcılara sadece, görevlerini gerçekleştirmek için gereken bilgilere (/uygulamalara) erişim verilir. (Farklı görevler/roller, farklı bilmesi gereken ve farklı erişim profili demektir.)	Ufuk Dikme
EKP-001-2.0		6.18. Daha zayıf kural olan “Açıkça yasaklanmadıkça her şeye izin verilir” kuralının aksine “Açıkça izin verilmedikçe her şey yasaklanır” kuralı geçerlidir.	Ufuk Dikme

Doküman Kod	İKÜ-BSTDB-EKP-001	Revizyon Tarihi	26.02.2022
Yayın Tarihi	02.10.2020	Revizyon No	EKP -001-2.0