İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI (BGYS)

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

Doküman Kod	IKU-BSTDB-BGYS-001	Revizyon Tarihi	21.02.2022
Yayın Tarihi	25.05.2020	Revizyon No	BGYS-001-2.0

İÇİNDEKİLER

1. AMAÇ

Bilgi Güvenliği Yönetim Sistemi politikası, T.C. İstanbul Kültür Üniversitesinin sahip olduğu hassas bilgi varlıklarının korunması ve yönetilebilmesi amacıyla TS ISO/IEC 27001 sayılı standarda uygun Bilgi Güvenliği Yönetim Sistemi kurulması ve bu sisteme ilişkin uygunluk belgesi alınması için uyulması gereken kuralları ortaya koyan bir belgedir. Kurumsal bilgi güvenliğinin sağlanmasına yönelik bir standart olan "ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı" belgesinin amacı; kapsam dâhilindeki bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlayarak, T.C. İstanbul Kültür Üniversitesi bünyesinde çalışanların ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kuralları belirlemektir.

2. KAPSAM

İşbu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde bulunan ve denetlenebilir nitelikte olan bilgi varlıklarını, bilişim sistemlerini, bunlara erişim sağlayan kullanıcıları ve ayrıca, sistem ve ağ altyapısı, yazılım geliştirme, malzeme ve hizmet tedariki ile bilgi güvenliği yönetimi iş süreçlerini kapsamaktadır.

Bilgi Güvenliği Yönetim Politikası, bilişim teknolojileri ile ilgili önlemlere ek olarak fiziksel ve çevresel güvenlik, insan kaynakları güvenliği, yasal mevzuata uyum ve üçüncü taraf ilişkilerinin yönetimi gibi birçok konuda çeşitli kontrollerin uygulanması ve belirli aralıklarla gözden geçirilmesi hususunda Bilgi Güvenliği Yönetim Sistemi çalışmalarının genel bir özetini teşkil etmektedir. Bu çalışmalarında üst belge niteliği taşıyan Bilgi Güvenliği Yönetim Sistemi Politikası, T.C. İstanbul Kültür Üniversitesinin Üst Yönetimi tarafından onaylanarak, T.C. İstanbul Kültür Üniversitesi personelinin bilgisine sunulmak ve üçüncü taraflara duyurulmak üzere yayınlanmaktadır. Bilgi Güvenliği Yönetim Sistemi Politikasında yapılacak güncellemeler Yönetimin Gözden Geçirme toplantılarında belirlenmekte ve Bilgi Güvenliği Yönetim Sistemi sorumluları tarafından dokümanlarda gerekli güncellemeler yapılarak T.C. İstanbul Kültür Üniversitesi Üst Yönetiminin onayına sunulmaktadır.

3. DAYANAK

- 24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.
- 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.
- 12.04.2018 tarihli 19924119-700-E.28137 sayılı Ulusal Strateji ve Eylem Planları konulu resmi yazı.
- 19.04.2019 tarihli 19924119-700-E.29445 sayılı Ulusal Strateji ve Eylem Planları konulu resmi yazı.
- 28.11.2019 tarihli 19924119-700-E.89576 sayılı "Ulusal Strateji ve Eylem Planları" konulu YÖK yazısında ise 13 Aralık 2019 tarihine kadar YÖKSİS üzerinden bu konuda gelinen noktanın raporlanması talep edilmiştir.

- 6 Temmuz 2019 tarih ve 30823 sayılı resmî gazetede 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konu başlıklı genelge.
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığının E-35030449-719-1758 sayılı Bilgi ve İletişim Güvenliği Rehberi konulu resmi yazısı.
- Cumhurbaşkanlığı tarafından yayımlanan 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" hakkında genelge.
- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğünün yayımladığı Kurumsal SOME Kurulum ve Yönetim Rehberi.
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin 5.2 Politika maddesi.

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.
BG İHLAL	İş operasyonlarını tehlikeye atma, bilgi akışını engelleme veya yavaşlatma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen/beklenmeyen olay ya da olayları ifade etmektedir
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
BÜTÜNLÜK	Bilginin yetkisiz değiştirmelerden korunması, değişiklik durumunda farkına varılması ve tüm birimler ve personel için ortak anlam taşımasını ifade etmektedir.
ERİŞİLEBİLİRLİK	Bilginin yetkilendirilmiş personel tarafından anlık olarak erişilebilmesini ifade etmektedir.
GİZLİLİK	Bilginin yalnızca yetkili personel tarafından erişebilir olması durumunu ifade etmektedir.
İKÜ	T.C. İstanbul Kültür Üniversitesi
YGG	Yönetimin Gözden Geçirmesi

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	IKU BSTDB BGYS Roller ve Sorumluluklar Dokümanı

2	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
3	IKU Organizasyon Şeması

6. BGYS HEDEFLERİ VE PRENSİPLERİ

BGYS Politikası, İKÜ çalışanları ve ilgili tarafların bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, personelin bilinç ve farkındalık seviyelerini artırmak ve bu şekilde İKÜ bünyesinde oluşabilecek riskleri asgari düzeye indirmek, İKÜ'nün itibarını ve bilgi güvenliği imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş gizlilik ve uygunluğu temin etmek, teknik açıdan bilgi güvenliği tedbirlerini almak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamayı hedeflemektedir.

BGYS kapsamındaki bilgi varlığı ve iş süreçlerinde gizlilik, bütünlük ve erişilebilirlik prensiplerine uygun tedbirler alınmasına istinaden, risk yönetimi faaliyetleri gerçekleştirilmektedir. Söz konusu risk yönetimi faaliyetlerinde amaç, İKÜ bünyesinde bulunan bilgi varlıkları için risk seviyesini kabul edilebilir risk seviyesinin altında tutmaktır. Risk yönetimi ve kontrollerin uygulanması dinamik bir BGYS sürecinin parçasıdır. Kabul edilebilir risk seviyesinin altında kalan bilgi varlıkları için de aksiyonlar atanarak iyileştirme çalışmaları yapılması amaçlanmaktadır.

Temel prensiplerimiz; Bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında ve risk değerlendirme metotları kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;

i. Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,
ii. Bilgi güvenliği ile ilgili tüm yasal mevzuata BGYS kılavuzu çerçevesinde uyum sağlamak,
iii. Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
iv. BGYS'yi sürekli gözden geçirmek ve iyileştirilmesi için BGYS'ye katkıda bulunmak,
v. Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirme vizyon ve misyonuyla hareket etmektedir.

7. BİLGİ GÜVENLİĞİ İLKELERİ

7.1. Bilgi güvenliği ilkeleri, İKÜ bilgi güvenliği ile ilgili genel kuralları ortaya koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.

7.2. Bilgi sistemleri ve teknolojileri altyapısını kullanan ve bilgi kaynaklarına erişen İKÜ Personeli:

i. Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
ii. Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
iii. Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,

iv. Bilgi güvenliği ihlal olaylarını Bilgi Güvenliği Yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.

7.3. İKÜ sahipliğindeki bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.

7.4. İKÜ bilişim kaynakları, T.C. Yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz.

7.5. İKÜ'nün tüm çalışanları; bu politika ile diğer desteklenen politikalara, prosedürlere ve talimatlarına, formlar ve sözleşme gerekliliklerine uymakla sorumludur.

7.6. İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.

7.7. Bilgilerin bütünlüğü her durumda korunacaktır.

7.8. Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.

7.9. BGYS'nin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.

7.10. Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.

8. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

Bu politika metninde belirtilen 1. ve 2. Madde de tarifi yapılan kapsam dâhilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Standartları gerekliliklerini yürütmek üzere İKÜ bünyesinde E-36253940-700-1084 ve E-89480013-700-1816 sayılı Makam Olurları ile bir BGYS Alt Komisyonu kurulmuştur. **Bu komisyon BGYS faaliyetlerini değerlendirmek üzere yılda 1 (Bir) kez toplanır.** BGYS Üst Yönetim, BGYS Yönetim Temsilcisi, BGYS Müdürü, Bilgi Varlığı Sahipleri, Risk Sahipleri, Daire Başkanları/Müdürler, Akademik/İdari Kadro ve Tarafların görev, yetki ve sorumlulukları "IKU BSTDB BGYS Roller ve Sorumluluklar Dokümanı" içerisinde tanımlanmıştır. Kurum organizasyon şemasına https://www.iku.edu.tr/tr/organizasyon-semasi adresi ya da "IKU Organizasyon Şeması" dokümanından ulaşılabilir.

BGYS ALT KOMİSYONU GÖREVLENDİRME TABLOSU

ADI	SOYADI	UNVANI	GÖREVİ
Prof. Dr. Hanife	Öztürk Akkartal	REKTÖR	Başkan
Dr. Öğr. Üyesi Elif	Altınok Çalışkan	REKTÖR DANIŞMANI	Başkan Yrd.
Ufuk	Dikme	CISO	Bilgi Güvenliği Yönetim Temsilcisi
Dr. Öğr. Üyesi İbrahim Ethem	Tarhan	GENEL SEKRETER	Başkan Yrd.

Serhat	Zorlu	IKDB	Üye
İsmail	Koç	BSTDB	Üye
Yusuf	Yılmaz	MİİDB	Üye
Sennur	Yılmaz	ÖİDB	Üye
Dr. Öğr. Üyesi Levent	Cuhacı	KBYDB	Üye
Yavuz İlker	Baldan	KİDB	Üye
Aynur	Candaş	SADB	Üye
Yasemin	Balcı	KDDB	Üye
Seçkin Taygun	Altıntaş	UİB	Üye
Dr. Dilek	Baykal	SKSDB	Üye
Seher	Türkdönmez	SRDB	Üye
Av. Kıvanç	Ayber	HUKUK MÜŞAVİRLİĞİ	Üye

9. BGYS POLİTİKASININ İHLALİ VE YAPTIRIMLARI

BGYS kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar için ilgili sözleşmelerde yer alan ve "T.C. İstanbul Kültür Üniversitesi Disiplin Politikası" dokümanında uygulamaları belirtilen aşağıdaki yaptırımlardan bir veya birden fazlasının uygulanması önerilebilir. Bu uygulamanın yürütülmesinden İKÜ Üst Yönetimi sorumludur.

- Kullanıcı sözlü ve/veya yazılı olarak uyarılır,
- Kullanıcıya tahsis edilmiş Bilişim Kaynakları sınırlı veya sınırsız süre ile kapatılabilir,
- Üniversite bünyesindeki akademik/idari soruşturma mekanizmaları harekete geçirilebilir,
- Adli yargı mekanizmaları harekete geçirilebilir,
- Sözleşme Feshi yapılabilir.

10. YÖNETİMİN TAAHHÜDÜ

T.C. İstanbul Kültür Üniversitesi Üst Yönetimi,

Tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan BGYS'ye uyulması, sistemin verimli şekilde çalışması ve bilgi güvenliği farkındalık programları düzenlenmesi için, imkânlar dâhilinde, gerek duyulan kaynakların tahsis edilmesini,

BGYS'nin etkinliğini, sürekli iyileştirilmesini ve bunun tüm İKÜ personeli tarafından anlaşılmasının sağlanmasını,

İKÜ personelinin ve üçüncü tarafların BGYS'ye katılımını ve uyumunu sağlamak için bilinçlendirici ve yönlendirici faaliyetler planlanmasının teşvik edilmesini,

BGYS özelinde hedefler belirlemeyi ve belirli dönemlerde uygunluklarını değerlendirerek, BGYS kapsamında risk yönetiminin gerçekleştirilmesini,

BGYS'nin gereksinimlerinin uygun olarak karşılanmasını, bilginin gizlilik, bütünlük ve erişilebilirlik unsurlarının korunmasını,

BGYS'nin yürütülmesi için kullanılan süreç ve faaliyetlerin sürekli iyileştirilmesi amacıyla belirli aralıklarla YGG toplantılarına iştirak edilmesini,

BGYS'nin gereği olan yasal mevzuata, sözleşme gereksinimlerine ve standartlara uyumun garanti altına alınmasını ve BGYS'nin kurum kültürümüzün vazgeçilmez bir parçası olarak uygulanmasının takip edilmesini taahhüt etmektedir.

İKÜ Üst Yönetimi olarak; BGYS Politikasının uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederiz

11. POLİTİKALAR

i. IKU BSTDB Ağ ve Ağ Hizmetlerine Erişim Politikası
ii. IKU BSTDB Bilgi Güvenliği Disiplin Politikası
iii. IKU BSTDB Bilgi Transfer Politikası
iv. IKU BSTDB Elektronik Posta Kullanım Politikası
v. IKU BSTDB Erişim Kontrol Politikası
vi. IKU BSTDB Felaket Kurtarma ve İş Sürekliliği Politikası
vii. IKU BSTDB Fikri Mülkiyet Hakları Uyum Politikası
viii. IKU BSTDB Güvenli Geliştirme Politikası
ix. IKU BSTDB İnsan Kaynakları Politikası
x. IKU BSTDB Internet Kullanım Politikası
xi. IKU BSTDB Mobil Cihaz ve Taşınabilir Ortam Kullanım Politikası
xii. IKU BSTDB Şifre Yönetimi Politikası
xiii. IKU BSTDB Tedarikçi İlişkileri Bilgi Güvenliği Politikası
xiv. IKU BSTDB Teknik Açıklık Politikası
xv. IKU BSTDB Temiz Masa Temiz Ekran Politikası
xvi. IKU BSTDB Uzaktan Erişim Politikası
xvii. IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası
xviii. IKU BSTDB Yardım Masası Yönetimi Politikası
xix. IKU BSTDB Yedekleme Politikası

xx. IKU KVKK Çerez Politikası

xxi. IKU KVKK Politikası

xxii. İstanbul Kültür Üniversitesi Web Sitesi Açma-Yayınlama İlke ve Esasları

12. PROSEDÜRLER

i. IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü

ii. IKU BSTDB Değişiklik Yönetimi Prosedürü

iii. IKU BSTDB Düzeltici İyileştirici Faaliyet Prosedürü

iv. IKU BSTDB İş Giriş Prosedürü

v. IKU BSTDB İşten Ayrılma Prosedürü

vi. IKU BSTDB Kapasite ve Performans Yönetim Prosedürü

vii. IKU BSTDB Mobil Cihaz ve Taşınabilir Ortam Kullanım Prosedürü

viii. IKU BSTDB Ortamın Güvenli Yok Edilme Prosedürü

ix. IKU BSTDB Personel Gizlilik Sözleşmesi

x. IKU BSTDB Sigorta Prosedürü

xi. IKU BSTDB Uzaktan Çalışma Prosedürü

xii. IKU BSTDB Yardım Masası Yönetimi Prosedürü

xiii. IKU BSTDB Yedekleme Prosedürü

13. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar
		8. Bu komisyon BGYS faaliyetlerini değerlendirmek üzere (yılda 1 (Bir) kez) ~~6 (Altı) ayda bir~~ toplanır.	