İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BGYS ROLLER VE SORUMLULUKLAR DOKÜMANI

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme		
Bilgi Güvenliği Yönetim Müdürü	BGYS Ekip Lideri	BGYS Koordinatörü

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

Doküman Kod	IKU-BSTDB-RSD-001	Revizyon Tarihi	
Yayın Tarihi	10.08.2020	Revizyon No	RSD-001-1.0

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

İÇİNDEKİLER

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

1. AMAÇ

Bu dokümanın amacı, BGYS rollerinin ve sorumluluklarının tanımlanarak BGYS sürecinin efektif şekilde yönetilmesidir.

2. KAPSAM

BGYS kapsam dokümanındaki tüm personeli, varlıkları ve ilişki içinde olunan 3.tarafları kapsar.

3. REFERANSLAR

ISO 27001:2013 Madde A.6.1.

4. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
İKÜ	T.C. İstanbul Kültür Üniversitesi
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
BGYS	Bilgi Güvenliği Yönetim Sistemi

5. SORUMLULUK VE YETKİ

GÖREV	ROLLER
Dokümanın Hazırlanması:	BSTDB Bilgi Güvenliği Yönetim Müdürü
Dokümanın Kontrolü:	BGYS Ekip Lideri
Dokümanın Onaylanması:	BGYS Koordinatörü
Dokümanın Yayınlanması:	BGYS Koordinatörü
Dokümanın Revizyonu:	BGYS Ekip Lideri
Dokümanın Uygulanması:	Tüm Personel
Dokümanın Yayından Kaldırılması:	BGYS Koordinatörü

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

6. UYGULAMA

6.1. BGYS Organizasyon Şeması

ROL	SAHİBİ
BGYS Koordinatörü	Rektör
BGYS Ekip Lideri	Kurumsal Bilgi Güvenliği Yöneticisi
BGYS Ekibi Üyeleri	

6.2. BGYS Görev Tanımları

6.2.1. ÜST YÖNETİM

a) İKÜ'nün stratejik amaçlarına uygun Bilgi Güvenliği Politikasını ve BGYS amaçlarını belirlemek.
b) BGYS kapsamındaki üst düzey dokümanları onaylamak, uygulamak ve yürürlükten kaldırmak.
c) BGYS'nin amaçlarına ulaşmak için gerekli olan tüm kaynakların ve sorumlulukların tahsislerini gerçekleştirmek, gerekirse yatırım yapmak.
d) BGYS'nin hedeflenen çıktılarına ulaşması, etkin bir BGYS kurulması, işletilmesi ve sürekli iyileştirilmesi için destek vermek.
e) Tüm çalışanları BGYS' ye katkı sağlaması için yönlendirmek ve motive etmek.
f) Kendisine yönlendirilen karar taleplerini karara bağlamak.
g) Uygun beceri ve niteliklerin sağlanmasında sürekliliğin temin edilmesi ve düzenli olarak eğitim verilmesinin teşvik edilmesi.
h) Bilgi güveliği politika ve prosedürleri ihlallerinin anonim bir raporlama kanalı ile raporlanmasının talep edilmesi.

6.2.2. BGYS KOORDİNATÖRÜ

a) Bilgi Güvenliği Yönetim Sistemi kurulmasını, işletilmesini ve sürekli iyileştirilmesini sağlamak/liderlik etmek.
b) BGYS'nin performansını izlemek ve sonuçları üst yönetime raporlamak.
c) ISO 27001 standartlarına uygun olarak Bilgi Güvenliği politikaları ve prosedürlerinin oluşturulmasını sağlamak.
d) Bilgi Güvenliği Yönetim Sistemi'nin Bilgi Güvenliği politikası ve hedefleri doğrultusunda uygulatılmasını sağlamak.
e) Bilgi Güvenliği Yönetim Sistemi kapsamında bilgi varlıkları envanterinin hazırlatılmasını sağlamak ve güncelliğini takip etmek.
f) Bilgi Güvenliği Yönetim Sistemi kapsamında BGYS müdürü tarafından yapılan risk analizleri sonucunda alınması gereken aksiyonları üst yönetime iletilmesini sağlamak.
g) Bilgi güvenliği performansını etkileyen çalışanların uygun yeterliliğe ulaşması için gerekli eğitimlerin alınmasını sağlamak.
h) Sorumlu olduğu BGYS dokümanlarını onaylamak, uygulatmak ve yürürlükten kaldırmak.
i) Çalışanların bilgi güvenliği farkındalıklarının artmasını sağlayacak mekanizmaların işletilmesini sağlamak.
j) Bilgi güvenliği ihlal olaylarını değerlendirmek ve takibini yapmak.
k) BGYS iç tetkikleri koordine etmek ve sonuçları değerlendirmek.
l) Üst yönetimin onaylayacağı Bilgi Güvenliği Yönetim Sistemi dokümantasyonunu kontrol etmek ve onaya sunmak.
m) Yönetim Gözden Geçirme Toplantısını organize etmek ve alınan kararların uygulatılmasını sağlamak.
n) Bilgi Güvenliği Yönetim Sistemi'nin işleyişi hakkında Üst Yönetime rapor vermek.

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

o) Tüm çalışmalarını ISO 27001 Standardı gerekliklerine göre hazırlanan ve yürürlüğe alınan dokümantasyonlara göre yürütmek.

p) Yasa, yönetmelik ve tüzükleri sürekli kontrol ederek ilgili değişiklikleri Üst Yönetime iletmek.

6.2.3. BGYS EKİP LİDERİ

a) Bilgi Güvenliği Yönetim Sistemi'nin kurulmasında, işletilmesinde ve sürekli iyileştirilmesi çalışmalarında görev almak.
b) Yaşanan Bilgi Güvenliği olaylarının SOME Ekibine bildirilmesini sağlamak.
c) Yaşanmış ve medyaya yansımış bilgi güvenliği olaylarının, farkındalık oluşturulması amacıyla Kurum çalışanlarına duyurulmasını sağlamak.
d) Bilgi Güvenliği Yönetim Sisteminin Bilgi Güvenliği politikası ve hedefleri doğrultusunda hazırlanmak ve uygulanmasını sağlamak.
e) Bilgi Güvenliği Yönetim Sistemi kapsamında bilgi varlıkları envanterini hazırlamak ve güncellemesini yapmak.
f) Bilgi Güvenliği Yönetim Sistemi kapsamında risk analizlerinin yapılması, değerlendirilmesi ve ilgili aksiyonların alınmasını sağlamak.
g) Bilgi Güvenliği Yönetim Sistemi'nin uygulatılması için gerekli faaliyetleri planlamak ve takip etmek.
h) Yönetim Gözden Geçirme toplantı tutanaklarıyla ilgili bilgileri toplantıya katılanlara ulaştırmak ve toplantılarda alınan kararların uygulanmasını sağlamak.
i) Bilgi Güvenliği Yönetim Sistemi'nin işleyişi hakkında Yönetim Temsilcisine rapor vermek.
j) BGYS farkındalık eğitimlerinin planlanmasını ve gerçekleştirilmesini sağlamak.
k) Bilgi Güvenliği Yönetim Sistemi kapsamında İç Denetimleri planlamak ve gerçekleştirilmesini sağlamak.
l) Bilgi Güvenliği Yönetim Sistemi kapsamında belirlenen uygunsuzluklar için düzeltici faaliyet formu düzenlemek, ilgili birimlere iletmek ve takibini yapmak.
m) Yasa, yönetmelik ve tüzükleri sürekli kontrol ederek ilgili değişiklikleri Yönetim Temsilcine iletmek.

6.3. BİLGİ VARLIĞI SAHİPLERİ

Bilgi varlığı ve bilgi varlığı operasyonel sahipleri, bilgi varlıklarının saklanması, işletilmesi, yönetilmesi, varlıklara erişim ve izleme kontrollerinin uygulanmasından sorumlu kişilerdir.
Bilgi varlığı ve bilgi varlığı operasyonel sahipleri BGYS politika ve prosedürlerine uygun olarak aşağıdaki kontrollerin uygulandığının kontrolünden sorumludur:

a) Fiziksel ve mantıksal (teknik) kontrollerin uygulanması.
b) Bilgi varlıklarına erişim yetkilerinin yönetilmesi.
c) Bilgi varlıklarına erişim yetkilerinin düzenli aralıklarla gözden geçirilmesi.
d) Bilgi varlıklarının sürekliliğinin sağlanması için uygun süreklilik ve kurtarma kontrollerinin uygulanması.

6.4. RİSK SAHİPLERİ

Risk sahibi, bir riski yönetmek için sorumluluk ve yetki verilmiş ve riskin azaltılması için aksiyon almaktan sorumlu kişi ya da kişilerdir. Risk sahibi aşağıdaki kontrollerden sorumludur.

a) Kendilerine görev olarak verilmiş riskleri gidermek veya giderilmesi için ilgililerle iletişime geçmek.

b) Riskin giderildiğinin kontrolünü yaparak kayıt altına almak.

c) Risk Yönetimi Prosedüründe belirtilen şekilde kabul edilebilir seviyedeki riskleri ve artık riskleri değerlendirip kabul etmek.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

6.5. DAİRE BAŞKANLARI/MÜDÜRLER

a) BGYS kapsamında hazırlanan politika, prosedür ve talimatların gerekliliklerinin birim çalışanları tarafından yerine getirilmesini sağlamak.

b) Birimine ait varlık envanteri ve risk analizi çalışmalarında yer almak ve sonuçları onaylamak.

c) Birimindeki çalışanların BGYS farkındalık eğitimlerini katılmasını sağlamak.

d) Biriminden ayrılan çalışanların (görev değişikliği, emeklilik, işten ayrılma vb.) fiziksel ve sistemsel erişim yetkilerinin durdurulmasını/kaldırılmasını sağlamak.

e) Kendisine bağlı birimde çalışacak üçüncü taraf bilgi sistemleri kullanıcılarının politikalardan ve prosedürlerden haberdar olmasını sağlamak.

f) Gereken durumlarda hizmet aldıkları 3.tarafların çalışanları ile bireysel gizlilik anlaşması imzalamak.

g) 3.taraflardan alınan hizmetlerin bilgi güvenliği ihtiyaçlarını değerlendirmek, bilgi güvenliğini sağlamak amacıyla kural ve şartlan belirlemek ve uygulatarak tedarik edilen ürün/hizmetin güvenli şekilde alınmasını sağlamak.

h) 3. Taraf firmalarla kurumsal gizlilik sözleşmesi imzalamak ve güncel tutmak.

i) Biriminde gerçekleşen tüm projelerin bilgi güvenliği açısından değerlendirilmesini sağlamak.

j) Görevler ayrılığı ilkesine göre çalışanların yetkilerini belirlemek.

k) İş sürekliliği ve felaketten kurtarma planlarını gözden geçirmek ve onaylamak.

6.6. AKADEMİK VE İDARİ KADRO

a) BGYS politika ve prosedürlerini bilmek ve uymak.

b) Bilgi varlıklarını bilgi varlığı sahibinin izin verdiği amaçla kullanmak.

c) 3. Bilgi varlığı sahibi ve bilgi varlığı operasyonel sahibinin belirlediği kontrollere uymak.

d) Erişilen bilgilerin bilgi sınıfına uygun biçimde gizliliğini sağlamak.

e) Farkındalık eğitimlerine katılmak.

f) Tespit edilen bilgi güvenliği ihlal olaylarını hemen ilgili prosedüre uygun olarak bildirmek.

g) İşten ayrılma durumunda kuruluşta çalışmakta olduğu süre boyunca kullanım için kendisine verilmiş olan ve kendisinin kuruluşta çalıştığı süre boyunca ürettiği tüm varlıkları kuruluşa teslim etmek.

6.7. TARAFLAR

a) İKÜ BGYS politika ve prosedürlerine uygun şekilde çalışmak.

b) BGYS'nin sağlıklı işlemesi için gerekli görülen önerileri ilgilisine iletmek.

c) Bilgi Güvenliği olaylarını, açıklıklarını ve ihlal durumlarını kuruluşa bildirmek.

d) Firma kuruluşta görevli çalışanlarının iş akdinin sonra ermesi durumunda, kuruluşun bina ve sistemlerine fiziksel ve mantıksal erişim yetkisi olan çalışanlarını zaman kaybetmeden kuruluşa bildirmek ve erişim yetkilerinin durdurulmasını/ kaldırılmasını sağlamak.

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.

6.8. ZİYARETÇİLER

Ziyaretçiler, "Ziyaretçilerin Uyması Gereken Kurallar" dokümanına uygun davranmakla yükümlüdür.

7. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

This document (including any attachments) is confidential and may be privileged. Any unauthorized use, copying, distribution or dissemination of this document in whole or in part is strictly prohibited. Bu döküman (ekleri de dahil olmak uzere) gizlidir ve imtiyazlı olabilir. Bu dökümanın bir kısmının veya tamamının izinsiz kullanımı, kopyalanması, dağıtımı veya kurum dışına sirayeti kesinlikle yasaktır. İstanbul Kültür Üniversitesi.