BGYS EL KİTABI

(ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EL KİTABI)

Yayın Geçmişi

Rev No	Revizyon Tarihi	Revizyon Nedeni	Hazırlayan	Onaylayan
00	07.09.2018	İlk Yayın	ÖZLEM EVRİM GÜNDOĞDU	EVREN KÖKSAL
01	17.10.2024	Güncelleme	Zerrin MERAL BGYS Üst Yönetim Temsilcisi	Evren KÖKSAL Daire Başkanı

	Adı, Soyadı	Ünvanı	İmza
Hazırlayan	Zerrin MERAL	BGYS Üst Yönetim Temsilcisi	
Gözden Geçiren/Onaylayan	Evren KÖKSAL	Daire Başkanı	

İçindekiler

1 Kapsam

Bu standart kuruluşun bağlamı dâhilinde bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları kapsar. Bu standart aynı zamanda kuruluşun ihtiyaçlarına göre düzenlenmiş bilgi güvenliği risklerinin değerlendirilmesi ve işlenmesi için şartları da içerir. Bu standartta ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm kuruluşlara uygulanabilir olması hedeflenmiştir. Bir kuruluşun bu standarda uyumluluk iddiasında bulunması durumda, Madde 4 ila Madde 10 arasında belirtilen şartların herhangi birinin hariç tutulması kabul edilebilir değildir.

2 Atıf yapılan standart ve/veya dokümanlar

Bu doküman genel olarak TS ISO/IEC 27001 (2022) standardında yer alan isterlere karşılık kurumun sağladığı BGYS ortamını tanımlamak için oluşturulmuştur.

Dolayısıyla doküman genel olarak TS ISO/IEC 27001 (2022) standardına atıfta bulunmaktadır.

TS ISO/IEC 27001 (2022) standardı içinde atıf yapılan standart ve dokümanlarda bu doküman tarafından dikkate alınmakta ve atıf yapılmaktadır.

Bunlara ek olarak doküman içinde, bu dokümanın bir parçası olan ve kurum içinde uygulanan BGYS yapısı esaslarını tanımlayan; politika, prosedür, talimat ve formlara atıfta bulunulabilmektedir.

Söz konusu atıflar dokümanın ilgili bölümlerinde verilmektedir. Eğer verilen atıflarda özel bir sürüm belirtilmemişse, dokümanın en güncel sürümü geçerlidir.

3 Terimler ve Tarifleri

BGYS: Bilgi Güvenliği Yönetim Sistemi

Varlık: Kuruluş için değeri olan herhangi bir şey.

Kullanılabilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği.

Bilgi güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

Bilgi güvenliği olayı: Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir ortaya çıkışı.

Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi güvenliği yönetim sistemi BGYS: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

Not - Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Artık risk: Risk işlemeden sonra kalan risktir.

Riskin kabulü: Bir riski kabul etme kararı.

Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımıdır.

Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses.

Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi.

Risk yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.

Risk işleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosesidir.

Uygulanabilirlik bildirgesi: Kuruluşun BGYS' si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirge.

Not - Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.

4 Kuruluşun Bağlamı

4.1 Kuruluşun bağlamının anlaşılması

TNKÜ BİDB'nin amacı ve stratejik yönü ile uygulamaya niyetlendiği Bilgi Güvenliği Yönetim Sisteminin amaçlanan sonucuna/sonuçlarına ulaşabilme yeteneğini etkileyen, iç ve dış hususlar aşağıda ele alınmıştır.

Bu hususlar iç ve dış hususlar olmak üzere iki başlık altında değerlendirilecektir.

4.1.1 İç Bağlam Değerlendirmesi

İç bağlamın anlaşılması; kuruluşun idari yapısı, değerleri, kültürü, bilgisi ve performansı ile ilgili hususların değerlendirilmesi dikkate alınarak yapılmaktadır.

TNKÜ BİDB Türkiye'nin en köklü ve büyük üniversitelerinden bir olan TNKÜ'nün bağlı birimlerinin bilgi işlem altyapısını kurmak ve işletlmekle sorumlu bir organizasyon olup bu işlevini uzun süredir yerine getirmektedir.

Kurumun idari yapısı, akademik anlamda tecrübesi bulunan Bilgi Güvenliği dahil uluslararası literatürde önem arz eden konulara hakim tecrübeli personellerden oluşmaktadır.

Bu kapsamda öncelikle hizmet sunulan taraflara ve sahip olduğu varlıklara önem atfetme konusu kurum kültürü açısından önemli bir yer tutmaktadır. Bu nedenle, kurum kültürü BGYS yapısının kurulması ve etkin bir şekilde yürütülmesi açısından katkı sağlayacaktır.

Kurum yönetimi BGYS süreçlerinin oturtulması konusunda niyetini ortaya koymuş ve bunun duyurusunu gerçekleştirmiştir. Buna ek olarak, süreçlerin oturtulmasında başta iş gücü (personel) olmak üzere kaynak ayrımını gerçekleştirmiştir.

TNKÜ BİDB Bilgi teknolojileri konusunda yetkin bir personel ve sistem altyapısına sahiptir. Söz konusu altyapının varlığı, kurumun operasyonel süreçlerde gösterdiği yüksek performansın BGYS süreçlerinin oturtulması ve işletilmesinde de katkı sağlayacaktır.

BGYS süreçlerinin uygulanması için iç bağlam açısından görülen tek olumsuz husus ülke genelinde Bilgi Güvenliği Konusunda insanlarda var olan farkındalık eksikliğinin TNKÜ BİDB personeline de yansımış olmasıdır. Personele sağlanacak farkındalık eğitimi ile bu olumsuzluk aşılmaya çalışılacaktır.

4.1.2 Dış Bağlam Değerlendirmesi

Dış bağlam değerlendirmesi; yasal, teknolojik, rekabetçi, pazar, kültürel, sosyal ve ekonomik çevrelerden (uluslararası, ulusal, bölgesel ve yerel olabilir) kaynaklanan hususların değerlendirilmesi ile yapılmıştır.

TNKÜ BİDB tarafından hizmet sunulan üniversite birimleri önemli verilere sahip olan kritik organizasyonlardır. Dolayısıyla, kendilerine hizmet sunan TNKÜ BİDB'den yüksek kalitede hizmet sunumu beklemektedirler. BGYS süreçlerinin kurum içinde oturtulması ve işletilmesi söz konusu şartlar gereği TNKÜ BİDB üzerinde baskı oluşturmaktadır.

TNKÜ BİDB başta Kişisel Verilerin Korunması Kanunu olmak üzere, kamu otoritelerine karşı yasal sorumlulukları vardır. Bu yasal sorumluluklar, kurumun BGYS gibi standartları uymasını gerekli kılmaktadır.

4.2 İlgili tarafların ihtiyaç beklentilerinin anlaşılması

TNKÜ BİDB faaliyetleri kapsamında ilgili taraflar ve beklentileri aşağıda listelenmiştir.

İlgili Taraf	İhtiyaç ve Beklenti
Kurum Üst Yönetimi	- Üst yönetimin kurum personelinden BGYS kapsamında tanımlanan şartlara uyması beklentisi mevcuttur. - Üst yönetimin ise, BGYS çalışmaları kapsamında gerekli kaynak ayrımını gerçekleştirmesi, yasal koyucuların şartlarının ve beklentilerinin belirlemesi ve karşılanması ve sürekli iyileştirilmesinin desteklenmesi beklenmektedir.
Kurum Personeli	- Kurum personeli, üst yönetim tarafından BGYS konusunda bilgilendirme ve farkındalığın sağlanmasına ihtiyacı vardır. - Kurum personeli, kişisel verilerinin kurum tarafından korunmasını beklemektedir. - Kurum personelinden, BGYS kapsamında tanımlanan şartlara uyması beklenmektedir.
Üniversite Birimleri	- Kuruma emanet ettikleri verilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını beklemektedir.
Akademik Kadro	- Kuruma emanet ettikleri verilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını beklemektedir.
Öğrenciler	- Kuruma emanet ettikleri verilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını beklemektedir.
Tedarikçiler ve Dış Kaynaklı Proses Tedarikçileri	- Kurum tedarikçlerinden kurumun bilgi güvenliği konusundaki hassasiyetini dikkate alarak kuruma hizmet sağlanması, gizlilik sözleşmesi şartlarına riayet edilmesini beklemektedir. - Kurumun tadarikçilerine bilgi güvenliği hakkında gerekli bilgilendirmeleri ve yönlendirmeleri yapması gerekmektedir.
Düzenleyici Kuruluşlar	- Belgelendirici kuruluş, kurumdan BGYS sertifikasyonu kapsamında gerekli kanıtarı sunmasını ve sertifikasyon sonrasında çalışmalarını - taahhüt edilen yönetim sistemi standartlarının uygun şekilde devam ettirmesini bekmektedir.
Bina Güvenliği Bina Yönetimi	- TNKÜ BİDB'ye yönetlik vandalizm, hırsızlık benzeri bir güvenlik tehdidi olduğunda müdahale etmek.
Kamu Otoriteleri (BTK)	- İnternet kullanım sisteminin 5651 sayılı kanun esaslarına uygun gerçekleştirilmesi
Kamu Otoriteleri (Kişisel verileri Koruma Kurulu)	- Kişisel verilerin 6698 sayılı Kişisel Verilerin Koruma kanunu uyarınca verilerin işlenmesi
Kamu Otoriteleri (YÖK)	- Faaliyetlerin Yüksek Öğrenim Kurumu tarafından belirlenen esaslara uygun olarak yürütülmesi

4.3 Bilgi Güvenliği Yönetim Sisteminin Kapsamı

BGYS tüm alt grupları ile beraber TNKÜ Bilgi İşlem Daire Başkanlığı tarafından işletilecektir. Bu alt gruplar TNKÜ BİDB içinde yer alan; Sistem ve Ağ Birimi, Yazılım Birimi, Teknik Servis Birimi, İdari İşler Birimi'dir.

Bilgi Güvenliği Yönetim Sistemi kapsamı aşağıda verilmiştir:

- Ağ ve sistem altyapısının kurularak sürekliliğinin sağlanması,
- Yazılım geliştirme, teknik servis, internet, eposta dahil bilişim sistemi altyapısının sürdürülmesi

4.4 Bilgi Güvenliği Yönetim Sistemi

Kurumumuz Bilgi Güvenliği Yönetim Sistemimiz ISO 27001:2022 standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde uygulamaktadır.

5 Liderlik

5.1 Liderlik ve Bağlılık

Üst yönetim aşağıdakileri sağlamak üzere liderlik ve bağlılık göstermektedir.

- BGYS faaliyetlerinde sponsorluk yapılması,
- BGYS politika ve amaçlarının kurumun strateji ve hedefleri ile uygun olmasının gözetilmesi,
- BGYS gereksinimlerinin organizasyon süreçlerine entegre olmasının sağlanması,
- BGYS için gerekli kaynağın ayrılması,
- BGYS'den beklenen çıktıların alınmasının sağlanması,
- Çalışanların BGYS'nin etkinliğine katkıda bulunması için onlara destek olmak ve yönlendirilmesi,
- Sürekli iyileştirmenin desteklenmesi,
- Kendi liderliklerini pekiştirmek için kendi sorumlulukları dahilinde ilgili yönetim rollerinin desteklenmesi.

5.2 Politika

Belirtilen kapsama uygun olarak Bilgi Güvenliği Politikası oluşturulmuştur.

İlgili Doküman

BİDB-PL.01 - BİLGİ GÜVENLİĞİ POLİTİKASI

5.3 Kurumsal Roller Sorumluluk ve Yetkiler

Üst yönetim tarafından bilgi güvenliği kapsamında roller ve sorumlular atamış, duyurusu yapılmıştır. Ayrıca bilgi güvenliği anlamında sorumluluğu olan veya BGYS içerisinde kendisine atıf yapılan tüm roller için görev tanımları yapılmıştır.

İlgili Doküman

BİDB-BGEK-EK-6.1-BİLGİ GÜVENLİĞİ EKİBİ ATAMA YAZISI
BİDB-BGEK-EK-6.2-BGYS YÖNETİM TEMSİLCİSİ ATAMA YAZISI
BİDB-BGEK-EK-6.3-BGYS YÖNETİCİSİ ATAMA YAZISI
BİDB-SM.01 – ORGANİZASYON ŞEMASI
BİDB-GT.02… - Görev Tanımları

6 Planlama

6.1 Bilgi Güvenliği Risk Değerlendirmesi

Bilgi güvenliği risk değerlendirme süreci tanımlanmıştır.

İlgili Doküman

BİDB-PR.09 – RİSK DEĞERLENDİRME PROSEDÜRÜ

6.2 Bilgi Güvenliği Amaçları ve Bu Amaçları Gerçekleştirmek İçin Planlama

Bilgi güvenliği hedefleri belirlenir ve her yılın sonuncu ayı içerisinde yapılan YGG toplantılarında sonuçları değerlendirilir.

İlgili Doküman

BİDB-PR.06 - YÖNETİMİN GÖZDEN GEÇİRME PROSEDÜRÜ
BİDB-PR.06-FR.01 HEDEF VE AKSİYON PLANI FORMU
BİDB-PR.06-FR.02 YGG TOPLANTI TUTANAĞI FORMU
BİDB-PR.06-FR.03 PERFORMANS RAPORU FORMU

7 Destek

7.1 Kaynaklar

Kurum yönetimi bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları belirlemekte ve sağlamaktadır.

7.2 Yeterlilik

Kurumumuzda yeterlilikler görev tanımlarında belirlenmiş ve yeterliliklerin gelişmesi yönünde ilgili prosedürler izlenmektedir.

İlgili Doküman

BİDB-GT.01… - Görev Tanımları
BİDB-PR.07 - İNSAN KAYNAKLARI VE EĞİTİM PROSEDÜRÜ
BİDB-PR.07 – FR.01 ORYANTASYON EĞİTİM FORMU
BİDB-PR.07 – FR.05 EĞİTİM KATILIM FORMU
BİDB-PR.07 – FR.03 YILLIK EĞİTİM PLANI FORMU
BİDB-PR.07 – FR.06 EĞİTİM DEĞERLENDİRME FORMU

7.3 Farkındalık

İlgili Doküman
BİDB-PR.07 - İNSAN KAYNAKLARI VE EĞİTİM PROSEDÜRÜ
BİDB-PR.07 – FR.01 ORYANTASYON EĞİTİM FORMU
BİDB-PR.07 – FR.05 EĞİTİM KATILIM FORMU
BİDB-PR.07 – FR.03 YILLIK EĞİTİM PLANI FORMU
BİDB-PR.07 – FR.06 EĞİTİM DEĞERLENDİRME FORMU

7.4 İletişim

Kurumumuz dahili ve harici iletişim kaynaklarını sağlamaktadır.

İlgili Doküman

BİDB-PR.14 – İLETİŞİM PROSEDÜRÜ

7.5 Yazılı Bilgiler

Kurumun oluşturduğu BGYS altyapısına ilişkin çıktılar dokümante edilmiştir. Bu dokümantasyonun yönetimi yapılmaktadır.

İlgili Doküman

BİDB-PR.01 – Doküman Kontrol Prosedürü

BİDB-PR.01 – FR.01 DOKÜMAN GÜNCEL LİSTESİ

BİDB-PR.01 – FR.04 DIŞ KAYNAKLI DÖKÜMAN LİSTESİ

BİDB-PR.02 – KAYITLARIN KONTROLÜ PROSEDÜRÜ

8 İşletim

Kurum bilgi güvenliği şartlarını karşılamak, bilgi güvenliği amaçlarına ulaşmak için sahip olduğu veya sorumluluğunda bulunan varlıkları tespit etmekte ve bunların risklerine yönelik çalışmalar yapmaktadır.

Bu kapsamda öncelikle, sahip olunan varlıklar taşıdıkları değerlere göre tespit edilmektedir. Bu varlıklar dikkate alınarak; riskler tespit edilmekte, analiz edilmekte ve işlenmektedir.

Risklerin durumu; varlıklara, BGYS'de yapılan değişikliklere, risklere yönelik yapılan çalışmalara bağlı olarak sürekli gözlemlenmektedir.

İlgili Doküman

BİDB-PR.08 - VARLIK ENVANTERİ HAZIRLAMA VE YÖNETİM PROSEDÜRÜ

BİDB-PR.09 – RİSK DEĞERLENDİRME PROSEDÜRÜ

BİDB-PR.08-FR.01 VARLIK ENVANTERİ FORMU

BİDB-PR.09-FR.01 RİSK DEĞERLENDİRME FORMU

BİDB-PR.09-FR.02 RİSK YÖNETİM PLANI FORMU

9 Performans Değerlendirme

9.1 İzleme Ölçme Analiz ve Değerlendirme

Bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliği takip edilmektedir.

İlgili Doküman

BİDB-PR.06 - YÖNETİMİN GÖZDEN GEÇİRME PROSEDÜRÜ
BİDB-PR.06-FR.01 HEDEF VE AKSİYON PLANI FORMU
BİDB-PR.06-FR.02 YGG TOPLANTI TUTANAĞI FORMU
BİDB-PR.06-FR.03 PERFORMANS RAPORU FORMU

9.2 İç Tetkik

Kurulan Bilgi Güvenliği Yönetim Sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler yılda en az bir kez yapılır. İç tetkiklerin nasıl gerçekleştirileceği İç Denetim Prosedüründe tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

İlgili Doküman

BİDB-PR.03 İÇ DENETİM PROSEDÜRÜ
BİDB-PR.03 – FR.01 İÇ DENETÇİ LİSTESİ FORMU
BİDB-PR.03 – FR.02 İÇ DENETİM PLANI FORMU
BİDB-PR.03 – FR.03 İÇ DENETİM SONUÇ RAPORU FORMU
BİDB-PR.03 – FR.04 İÇ DENETİM SORU LİSTESİ

9.3 Yönetimin Gözden Geçirme

Kurumumuz BGYS'yi ***yılda en az bir kez***, sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirmektedir. Bu gözden geçirme, bilgi güvenliği politikası ve bilgi güvenliği amaçları dâhil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini içermektedir. Gözden geçirme sonuçları açıkça dokümante edilmekte ve kayıtlar tutulup saklanmaktadır.

Gözden Geçirme Girdisi

Yönetimin gözden geçirmesinin girdileri aşağıdakileri içermektedir:

- BGYS denetimleri ve gözden geçirmelerinin sonuçları,
- Bilgi güvenliğini ilgilendiren iç ve dış konulardaki değişiklikler,
- Bilgi güvenliği performansına dair geri bildirim (Uygunsuzluk ve Düzeltici Faaliyetler, İzleme Ölçme Sonuçları, tetkik sonuçları, bilgi güvenliği amaç ve hedefleri)
- İlgili taraflardan edinilen geri bildirimler,
- Risk değerlendirme sonuçları ve risk işleme planının durumu,
- Sürekli İyileştirme İçin Fırsatlar

İlgili Doküman

BİDB-PR.06 – YÖNETİM GÖZDEN GEÇİRME PROSEDÜRÜ

10 İyileştirme

10.1 Uygunsuzluk Düzeltici Faaliyet

Kurum, bir uygunsuzluk meydana geldiğinde; bunları sistemli olarak çözmek, uygunsuzlukları takip etmek ve tekrarını engellemek için yazılı prosedürler tanımlamıştır.

Düzeltici faaliyet için dokümante edilmiş prosedür (P.04 DF Prosedürü) aşağıdaki gereksinimleri tanımlamaktadır;

- Uygunsuzlukları tanımlama,
- Uygunsuzlukların nedenlerini belirleme,
- Uygunsuzlukların tekrarlanmamasını sağlamak için ihtiyaç duyulan faaliyetleri değerlendirme,
- Gereken düzeltici faaliyetleri belirleme ve gerçekleştirme,
- Gerçekleştirilen faaliyetlerin sonuçlarını kaydetme
- Gerçekleştirilen düzeltici faaliyetleri gözden geçirme.

İlgili Doküman

BİDB-PR.04 DÜZELTİCİ FAALİYET PROSEDÜRÜ

10.2 Sürekli İyileştirme

Kurumumuz bilgi güvenliği politikasını, güvenlik amaçlarını, denetim sonuçlarını, izlenen olayların analizini, düzeltici ve önleyici faaliyetleri ve yönetimin gözden geçirmelerini kullanarak BGYS etkinliğini sürekli iyileştirmektedir.

İlgili Doküman

BİDB-PR.03 İÇ DENETİM PROSEDÜRÜ

BİDB-PR.04 DÜZELTİCİ FAALİYET PROSEDÜRÜ

BİDB-PR.06 YÖNETİMİN GÖZDEN GEÇİRME PROSEDÜRÜ

BİDB-PR.07 İNSAN KAYNAKLARI VE EĞİTİM PROSEDÜRÜ