DAİRE

daire, yazı tipi, grafik, logo içeren bir resim

Açıklama otomatik olarak oluşturuldu

**BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ**

**BİLGİ İŞLEM DAİRE BAŞKANLIĞI**

**BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EL KİTABI**

yazı tipi, metin, logo, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu



C

İÇİNDEKİLER

[0. GİRİŞ 3](#_Toc137641557)

[0.1. Genel 3](#_Toc137641558)

[1. AMAÇ 5](#_Toc137641559)

[2. KAPSAM 5](#_Toc137641560)

[2.1. Belgelendirme Kapsamı 5](#_Toc137641561)

[3. ATIF YAPILAN STANDARTLAR 5](#_Toc137641562)

[4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ 6](#_Toc137641563)

[4.1. Kuruluşun ve Bağlamının Anlaşılması 6](#_Toc137641564)

[4.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması 7](#_Toc137641565)

[4.3. Bilgi Güvenliği Yönetim Sisteminin Kapsamının Belirlenmesi 7](#_Toc137641566)

[4.4. Bilgi Güvenliği Yönetim Sistemi 7](#_Toc137641567)

[5. LİDERLİK 8](#_Toc137641568)

[5.1. Liderlik ve Bağlılık 8](#_Toc137641569)

[5.2. Politika 9](#_Toc137641570)

[5.3. Kurumsal Roller, Sorumluluklar ve Yetkiler 9](#_Toc137641571)

[6. PLANLAMA 9](#_Toc137641572)

[6.1. Risk ve Fırsatları Ele Alan Faaliyetler 9](#_Toc137641573)

[6.1.1. Genel 9](#_Toc137641574)

[6.1.2. Bilgi Güvenliği Risk Değerlendirmesi 9](#_Toc137641575)

[6.1.3. Bilgi Güvenliği Risk İşleme 11](#_Toc137641576)

[6.2. Bilgi Güvenliği Amaçları ve Bu Amaçları Başarmak İçin Planlama 12](#_Toc137641577)

[7. DESTEK 12](#_Toc137641578)

[7.1. Kaynaklar 12](#_Toc137641579)

[7.2. Yeterlilik 12](#_Toc137641580)

[7.3. Farkındalık 13](#_Toc137641581)

[7.4. İletişim 13](#_Toc137641582)

[7.5. Yazılı Bilgiler 14](#_Toc137641583)

[7.5.1. Genel 14](#_Toc137641584)

[7.5.2. Oluşturma ve Güncelleme 14](#_Toc137641585)

[7.5.3. Yazılı Bilgilerin Kontrolü 14](#_Toc137641586)

[8. İŞLETİM 15](#_Toc137641587)

[8.1. İşletimsel Planlama ve Kontrol 15](#_Toc137641588)

[8.2. Bilgi Güvenliği Risk Değerlendirme 15](#_Toc137641589)

[8.3. Bilgi Güvenliği Risk İşleme 15](#_Toc137641590)

[9. PERFORMANS DEĞERLENDİRME 16](#_Toc137641591)

[9.1. İzleme, Ölçme, Analiz ve Değerlendirme 16](#_Toc137641592)

[9.2. İç Tetkik 16](#_Toc137641593)

[9.3. Yönetimin Gözden Geçirilmesi 17](#_Toc137641594)

[10. İyileştirme 18](#_Toc137641595)

[10.1. Uygunsuzluk ve Düzeltici Faaliyet 18](#_Toc137641596)

[10.2. Sürekli İyileştirme 18](#_Toc137641597)

[EK-1 : BGYS İŞ AKIŞI 19](#_Toc137641598)

[EK-2: BGYS STANDART MADDESİ İLE DOKÜMAN EŞLEŞTİRMESİ 20](#_Toc137641599)

# GİRİŞ

## Genel

Bilgi, kurum/kuruluşların günlük işlerinin, kayıtlarının ve birikimlerinin sonucu elde edilen ve karar verme aşamasında da kullanılabilen islenmiş veya işlenmemiş veri anlamına gelmektedir. Güvenlik ise, can ve mal varlıklarının her türlü tehdit ve tehlikelerden korunması seklinde tanımlanabilir. Bu iki tanımdan hareket ederek bilgi güvenliğini, verinin, toplanması, son kullanıcıya ulaşması, saklanması ve kullanımı aşamalarında her türlü tehdit ve tehlikelerden korunması, bu amaçla önceden alınacak tedbirler ve saldırı halinde yapılabilecek işlemlerin tümünü kapsayan bir disiplin olarak tanımlayabiliriz.

Bilgi güvenliğinin ana amacı, her türlü ortamdaki (basılı, elektronik vb.) verinin güvenliğini sağlamak, veri bütünlüğünü korumak ve veriye erişimi denetleyerek gizliliği ve sistem devamlılığını sağlamaktır. Burada önemli bir husus da güvenliğin kullanıcıya aşırı sınırlamalar getirmeden ancak, kullanıcı tercihlerinden de bağımsız olarak sağlanmasıdır.

İyi bir bilgi güvenliği, bütün güvenlik çözümlerinin bir araya getirilmesiyle oluşur. Dolayısıyla, bilginin güvenliğini sağlamak için birden çok güvenlik çözümüne ihtiyaç vardır. Tek bir güvenlik çözümü veri ve bilgisayar sistemlerinin güvenliğini tam olarak sağlayamaz ve yeterli bir güvenlik sistemi olarak düşünülemez.

Bilgi güvenliği her türlü ortamda tutulan verilerin, programların ve her türlü bilginin korunması anlamına gelmektedir. Bilgi güvenliğinin temel amaçları Gizlilik, Bütünlük, Erişebilirlik, İnkâr edememe ve İzleme olarak verilebilir.

# AMAÇ

Bilgi Güvenliği El Kitabının amacı Bandırma Onyedi Eylül Üniversitesi’nin bilgi güvenliği seviyesini sürekli iyileştirmek, yaşanabilecek bilgi güvenliği olaylarına zamanında ve etkili biçimde yanıt verebilmek için uyguladığı yönetim sistemini ISO 27001 standardına paralel olarak tanımlamak, ilgili politika, prosedür ve kayıtlara referans vererek yönetim sisteminin bütününü oluşturan bu parçaların yönetim sistemindeki yerlerini ifade etmektir.

# KAPSAM

Bandırma Onyedi Eylül Üniversitesi için kurulan ve işletilen bilgi güvenliği yönetim sistemi, insan, alt yapı, yazılım, donanım, müşteri bilgileri, şirket bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar olarak sınıflandırdığımız varlıkların tamamını kapsar.

Bu varlıklarla ilgili her türlü ortamda saklanan fiziksel ve sanal bilgiler ve bu ortamlar BGYS kuralları dahilinde korunur ve sistem sürekliliği takip edilir.

Bandırma Onyedi Eylül Üniversitesi Bilgi İşlem Daire Başkanlığı Tarafından Yürütülen Bilgi İşlem Faaliyetlerinin Bilgi Güvenliği Hizmetleri sunar ve tüm operasyonları ISO 27001 BGYS kapsamı içindedir.

Kapsam faaliyetlerimizi gerçekleştirirken kullandığımız dış kaynaklı prosesler;

Yazılım Geliştirme Faaliyetleri tedarikçi firma tarafından yapılmakta olup 3. Taraf Gizlilik Sözleşmeleri ile süreç güvence altına alınmaktadır. Yapılan tüm işlemler sırasında Bilgi Güvenliği Ekibi tarafından refakat edilmekte ve izleme uygulamaları ile kayıt altına alınmaktadır.

## Belgelendirme Kapsamı

Bandırma Onyedi Eylül Üniversitesi Bilgi İşlem Daire Başkanlığı Tarafından Yürütülen Bilgi İşlem Faaliyetlerinin Bilgi Güvenliği Hizmetleri faaliyetlerini kapsamaktadır.

# ATIF YAPILAN STANDARTLAR

Bandırma Onyedi Eylül Üniversitesi Bilgi Güvenliği Yönetim Sisteminin oluşturulmasında TS EN ISO 27001:2022 referans standart alınarak hazırlanmıştır.

# BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

## Kuruluşun ve Bağlamının Anlaşılması

Kurumun vermeyi taahhüt ettiği hizmetlerde, yasal ve mevzuat şartlarının gerektirdiği düzeyde Bilgi Güvenliği faaliyetlerini yürütmeyi hedeflemektedir. Herhangi bir istenmeyen bilgi güvenliği riskleri için Risk değerlendirme Prosedürü’nde tanımlanan önceden belirlenen risklerin bertaraf edilmesi hedeflemektedir.

Bu anlamda Kurumun hizmet verme kapasitesini belirleyen, etkileyen iç ve dış konular şunlardır:

* Kamusal kaynaklardan edinilen, telefon, internet, elektrik, su, doğalgaz, kanalizasyon vb. konular,
* İç ve dış kaynaklardan sağlanan personel,
* Tedarikçilerden alınan hizmetler,
* Kurumun ortakları,
* Kurumun alt yapısı ve teknolojik olanakları,
* Finansal kaynaklı konular.
* Güvenlik hizmetleri

Yukarıda belirtilen konular Kurumun bünyesinde BGYS’ni oluştururken, uygularken ve sürdürürken göz önünde bulundurulmakta ve sürekli gözden geçirilmektedir.

Kurumun yapısı,

1. BGYS Ekibi tarafından yapılan Değerlendirme toplantılarında, Kurumun faaliyetleri, fonksiyonları, hizmetleri, ürünleri, ortaklıkları, tedarik zincirleri, ilgili taraflar ile ilişkileri ve bilgi güvenliği olaylarına yol açan bir durum ile ilgili potansiyel etkiler tanımlanmış ve ortaya çıkartılan konular doğrultusunda Varlık Envanteri ve Risk Değerlendirme Tablosunda dokümante edilmiştir.

b) Kurumun Risk Yönetim Stratejisi, potansiyel riskler dahil Kritiklik Seviyeleri vb. hususlar **Risk Yönetim Prosedürü**nde açıkça ifade edilmiştir.

Bilgi Güvenliği İçeriği/Yapısı belirlenirken Kurumun aşağıdakileri yerine getirmiştir:

1) Bilgi Güvenliği ile ilgili olanlar dahil hedefler belirlenmiş ve ilgili taraflara duyurulmuş,

2) Riske neden olan belirsizlikleri yaratan dahili ve harici faktörler tanımlanmış,

3) Kurumun risk potansiyeli göz önünde bulundurarak risk kriterleri belirlenmiş,

4) BGYS’nin amacı tanımlanmıştır.

**Referanslar:**

Risk Yönetim Prosedürü

Varlık Envanteri ve Risk Değerlendirme Tablosu

KURULUŞ, STRATEJİK YÖNÜNE VE AMACINA ETKİ EDEN İÇ VE DIŞ KONULAR

## İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

Kurumun BGYS’ni kurarken, tüm paydaşların ihtiyaç ve beklentileri yasal ve mevzuat şartları açısından ve hizmetin gerektirdiği şartlar açısından, Bilgi Güvenliği Ekibi tarafından yapılan **Risk Değerlendirme toplantıları** ile gözden geçirilmiş ve Varlık Envanteri ve Risk Değerlendirme Tablosunda tüm ilgili riskler, etkileriyle birlikte tanımlanmıştır.

**Referanslar:**

Varlık Envanteri ve Risk Değerlendirme Tablosu

## Bilgi Güvenliği Yönetim Sisteminin Kapsamının Belirlenmesi

Kurumun BGYS’nin kapsamını, sınırlarını ve uygulanabilirliğini belirlerken, **BGYS Ekibi Değerlendirme Toplantıları**ndan çıkan sonuçlardan yararlanmış tüm ilgili tarafların ihtiyaç ve beklentilerini dikkate almıştır.

Kapsama ait bilgiler bu el kitabının Kapsam bölümünde paylaşılmıştır.

Kurumun kapsam bölümünde;

a) BGYS kapsamında yer alacak olan organizasyon bölümlerini belirlemiş,

b) Kurumun misyonunu, hedeflerini, dahili ve harici yükümlülüklerini (ilgili taraflar ile ilgili olanlar dahil) ve yasal ve düzenleyici sorumlulukları göz ününde bulundurarak BGYS şartlarını belirlemiş,

c) BGYS kapsamında yer alan ürün ve hizmetleri ve tüm ilgili faaliyetleri tanımlamış,

d) İlgili tarafların ihtiyaç ve beklentilerini dikkate almış (müşteriler, ortaklar, tedarikçiler, iş ortakları) ve

e) BGYS kapsamını Kurumun büyüklüğüne, yapısına ve karmaşıklığına göre tanımlamıştır.

Kurumun kapsam dışında tutulan alan, bölüm, organizasyon ve faaliyete yönelik bilgileri paylaşmış, herhangi bir hariç tutmada bunu gerekçeleri ile birlikte açıklamıştır.

Söz konusu kapsam dışı bırakma, risk değerlendirmesi ve geçerli yasal veya düzenleyici koşullar ile belirlendiği şekilde; BGYS şartlarını sağlayan iş ve operasyonların gizlilik, bütünlük ve sürekliliğini sağlamak için kuruluşun kapasite ve sorumluluklarını etkilememesi temelinde uygulanmasına dikkat edilmiştir.

**Referanslar:**

UYGULANABİLİRLİK BİLDİRGESİ

KAPSAM VE SINIRLAR PROSEDÜRÜ

## Bilgi Güvenliği Yönetim Sistemi

BGYS kapsamında oluşturulan tüm dokümanlar ortak alana konulmuş ve personel erişimine açılmıştır. Kapsam faaliyetlerimizi gerçekleştirirken karşılaşabilecek tüm riskler varlık envanteri ve risk değerlendirme tablosu içerisinde ele alınmış olup, risk izleme sayfası üzerinden tespit edilen risklerin takibi yapılmaktadır. Kurumun ISO 27001 standardı paralelinde ihtiyaç duyulan prosesler ve bunların etkileşimi dahil bir BGYS oluşturmuş, oluşturulan BGYS kurallarını uygulamakta, sürdürmekte ve sürekli olarak iyileştirmektedir.

**Referanslar:**

EK- 1: BGYS İş Akışı Tablosu

## LİDERLİK

## Liderlik ve Bağlılık

Kurumun Üst yönetimi BGYS kurulmasında ve uygulanmasında liderlik etmekte, BGYS uygulamalarına üst düzeyde katılım sağlamaktadır.

Üst Yönetim kendi içinde, BGYS kurulmasında ve uygulanmasında görev alacak BGYS Temsilcisi ataması olarak bilgi güvenliği departmanı oluşturmuştur

**Yönetim Taahhüdü**

Kurumun Üst Yönetimi, aşağıdakileri yerine getirerek BGYS ile ilgili liderlik ve taahhüdünü göstermektedir:

Bu doğrultuda kurumun Üst Yönetimi:

— politika ve hedeflerin Bilgi Güvenliği yönetim sistemi için oluşturulmasını ve kurumun stratejik yönelimi ile uyumlu olmasını sağlamakta,

— Bilgi Güvenliği yönetim sistemi şartlarının kurumun iş süreçlerine entegrasyonu için çaba harcamakta,

— Bilgi Güvenliği yönetim sistemi için ihtiyaç duyulan personel, finansal, teknolojik ve bilgi kaynaklarının bulunmasını sağlamakta,

— Yapılan toplantı, eğitim, panel vb. her fırsatta etkili bir Bilgi Güvenliği yönetim sisteminin önemine vurgu yapmakta ve BGYS şartlarına üst düzeyde uymakta,

— BGYS’nin hedeflenen sonuçları elde etmesi için çalışmakta,

— Çalışanları ve ilgili tarafları BGYS’nin etkinliğine katkıda bulunmaları için yönlendirmekte ve desteklemekte,

— Sürekli iyileştirmeyi teşvik etmekte ve

— Yönetimin görevlendirdiği diğer yöneticilerin çalışmalarını desteklemektedir.

Üst yönetim BGYS’nin uygulanmasındaki yükümlülüğünün gereğini,

— Bir “**Bilgi Güvenliği Politikası”** belirleyerek,

— **“Bilgi Güvenliği Hedeflerinin Hedef Takip Tablosu”** ndabelirlenmesini sağlayarak,

— Bilgi Güvenliği Yönetimi için **Görevleri, Sorumlulukları Ve Yeterlilikleri** belirleyerek ve

— BGYS’nin uygulanmasında ve devam ettirilmesinde tanımlanacak olan doğru yetki ve yeterliliğe sahip BGYS Koordinatörü atayarak yerine getirmektedir.

Kurumun Üst yönetiminin BGYS ile ilgili temel görevleri aşağıdaki gibi özetlenebilir:

— “**Risk Yönetimi Prosedürü”** ne uygun olarak, riskleri kabul etme ve kabul edilebilir risk seviyeleri için kriterler tanımlama,

— “**İş Sürekliliği ve Acil Durum Yönetimi Prosedürü**” ne uygun olarak, uygulama ve test etme/tatbikatlara aktif bir şekilde katılma,

— BGYS’nin “**İç Tetkik Prosedürü”** ne uygun olarak iç denetimlerinin yapılmasını sağlamak,

— BGYS’nin “**YGG Prosedürü”** ne uygun olarak yönetim gözden geçirmelerini yürütmek ve

— Sürekli iyileştirme taahhüdünü göstermek.

**Referanslar:**

Bilgi Güvenliği Politikası

Görev Tanımları

Risk Yönetimi Prosedürü

İş Sürekliliği ve Acil Durum Yönetimi Prosedürü

İç Tetkik Prosedürü

YGG Prosedürü

Hedef Takip Tablosu

## Politika

Kurum Üst yönetimi:

a) Kurumun kuruluş amacına uygun olan,

b) Bilgi Güvenliği hedeflerinin belirlemek için bir çerçeve sunan,

c) Uygulanabilir koşulları yerine getirme taahhüdünü içeren,

d) BGYS’nin sürekli gelişme taahhüdünü içeren.

Bir BGYS politikası belirlemiş ve dokümante etmiştir. Bu politika Firma içerisinde uygun iletişim kanalları ile tüm çalışanlara ve ilgili taraflara duyurulmakta, YGG toplantılarında ve önemli değişiklikler olduğunda uygunluk için sürekli gözden geçirilmektedir.

**Referanslar:**

Bilgi Güvenliği Politikası

## Kurumsal Roller, Sorumluluklar ve Yetkiler

Kurumun, Üst Yönetimi, BGYS ile ilgili görevler için sorumlu ve yetkililerin atanmasını sağlamakta ve bunun kurum içinde uygun iletişim kanalları ile duyurulmasını sağlamaktadır.

**Referanslar:**

Görev Tanımları

## PLANLAMA

## Risk ve Fırsatları Ele Alan Faaliyetler

## Genel

Kurum BGYS ile ilgili planlama yaparken, daha önceden yapılan Risk analizi ve ilgili tarafların beklentilerini göz önünde bulundurmaktadır.

Kurumun Üst Yönetimi, BGYS’nin hedeflenen çıktılara ulaşmasını sağlamak, istenmeyen sonuçları önlemek veya azaltmak ve sürekli iyileştirmeyi sağlamak için belirlenen Risklere ve muhtemel fırsatlara yönelik olarak planlama “**Varlık Envanteri ve Risk Değerlendirme Listesi**” nde yapmaktadır. Kurumun bünyesindeki riskler ve fırsatlara yönelik alınan tedbirlere Bilgi Güvenliğine yönelik planları, gerektiğinde oluşturulan proses/prosedürler, talimatlar ile operasyonel olarak kontrol etmekte ve sonuçlarını “**Risk Yönetim Prosedürü”** ne göre değerlendirmektedir.

**Referanslar:**

Varlık Envanteri ve Risk Değerlendirme Tablosu

Risk Yönetim Prosedürü

## Bilgi Güvenliği Risk Değerlendirmesi

Bilgi güvenliği yönetim sisteminin kapsamı tüm kuruluşumuzun organizasyonu, yerleşkeleri ve süreçlerinden oluşmaktadır. Kapsamın bağımlılıkları, sınırları ve ara yüzleri Kapsam ve Sınırlar dokümanında detaylı biçimde açıklanmıştır.

**Referanslar:**

Kapsam ve Sınırlar

Risk değerlendirme yaklaşımı iş ve yasal düzenlemelerden kaynaklanan gereksinimlerin varlık envanterinin oluşturulması safhasında belirlenmesini temin edecek biçimde geliştirilmiş ve uygulanmaktadır. Risk kabul kriterleri ve kabul edilebilir risk seviyeleri **"Risk Yönetim Prosedürü”** nde ifade edilmiştir. Tanımlanan risk değerlendirme metodolojisi ISO 31000 standardı esas alınarak hazırlanmış olup karşılaştırılabilir ve yeniden üretilebilir değerlendirme sonuçlarının üretilmesini destekleyecek niteliktedir.

**Referanslar:**

Risk Yönetim Prosedürü

BGYS kapsamında bulunan bilgi varlıkları risk profilleri dikkate alınarak risk analizini pratik kılacak gruplar halinde dokümante edilir. Bilgi varlıklarının sahipleri tanımlanır. Her bir varlık (veya gruplanmış varlık) için gizlilik, bütünlük ve erişilebilirlik değerleri bir bilgi güvenliği riskinin gerçekleşmesi durumunda oluşabilecek etkiler değerlendirilerek belirlenir. Bilgi varlıklarına yönelik tehditler, oluşturulmuş olan tehdit listesindeki tehditler gözden geçirilerek ancak bu tehditlerle kısıtlı kalmadan değerlendirilir. Her bir varlık tehdit çifti için risk doğurabilecek açıklıklar belirlenir.

**Referanslar:**

Varlık Envanteri ve Risk Değerlendirme Tablosu

Olası risk senaryosu bazında Bilgi Güvenliği **"Risk Yönetimi Prosedürü**” nde belirtildiği üzere her bir varlık - tehdit - zafiyet üçlüsü için; tehdidin olumsuz etkileyebileceği varlık bilgi güvenliği ihtiyaçları (gizlilik, bütünlük, erişilebilirlik) belirlenir. Tehdit olasılığı tehdidin geçmişte yaşanma deneyimine, mevcut konjönktüre ve varlığın konum ve niteliğine bağlı olarak tahmin edilir. Zafiyet düzeyi ilgili risk senaryosu için geçerli bilgi güvenliği kontrollerinin yeterliliği ve varlığın içsel özellikleri dikkate alınarak tahmin edilir. Tüm bu faktörler "Risk Yönetimi Prosedürü ’nde belirtilen ölçekler kullanılarak sayısallaştırılır ve prosedürde belirtilen sayısal formüller kullanılarak risk büyüklükleri hesaplanır. Risk değerlerinin hesaplanması sonrasında kabul edilebilir ve edilemez riskler ayrıştırılır.

**Referanslar:**

Risk Yönetim Prosedürü

Belirlenen risklere karşı izlenecek strateji her bir risk için ISO 27001 standardında belirtilen 4 strateji arasından seçilir. Riskin azaltılması veya ortadan kaldırılması için öncelikle kabul edilebilir seviye üzerindeki riskler ele alınır, ancak maliyet olarak etkin kontrollerin uygulanabileceği kabul edilebilir seviyedeki riskler için de gerekli kontroller uygulanabilir.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

## Bilgi Güvenliği Risk İşleme

Her bir risk ile ilgili ISO 27002 kontrolleri risk değerlendirme tablosunda ve Risk İşleme Planında belirtilir. Risk işleme planı varlık envanteri ve risk değerlendirme tablosu içerisinde ayrı bir sayfada tanımlanmıştır.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

Risk Değerlendirme Tablosu’nda seçilen risk stratejisi ve uygulanması planlanan risk işleme planı sonrasında hedeflenen artık risk değerleri değişmesi planlanan tehdit olasılığı ve zafiyet düzeyine bağlı olarak hesaplanır. Yönetime yapılan bir sunum ile risk değerlendirmesi ve risk işleme planı ile ilgili yönetimin görüşü alınır ve artık risklerin resmen onaylanması sağlanır.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Listesi

Artık Risk Onay Tutanağı

Risk işleme planının gerçekleştirilmesi için BGYS Ekibi desteği ile BGYS Koordinatörü koordinasyonunda ilgili kontrol sorumluları ile birlikte risk işleme planı statüsü takip edilir.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

Standardın gereklerine uygun olarak "Uygulanabilirlik Bildirgesi" hazırlanır / güncellenir, mevcut ve uygulanması planlanan kontroller belirtilir, uygulanabilir olmayan ISO 27002 kontrolleri için uygulanabilir olmama gerekçeleri dokümante edilir. Uygulanabilirlik bildirgesinde daha önceden mevcut olmayan veya bir riski azaltmak için iyileştirilmesi gereken kontroller ilgili oldukları risk maddeleri ile ilişkilendirilerek seçilme gerekçeleri dokümante edilir.

Referanslar:

Uygulanabilirlik Bildirgesi

Risk işleme planına dahil edilen kontroller, Düzeltici Faaliyet Planı'na dahil edilir, hedeflenen bitiş tarihleri ve sorumluları belirlenir. Uygulanması için maddi kaynak gereken kontroller için kurumsal bütçeleme süreci işletilerek gerekli kaynaklar bütçelenir. Risk işleme planı ve diğer düzeltici faaliyetlerin uygulanması BGYS Koordinatörü koordinasyonunda ilgili yöneticiler tarafından takip edilir.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

Düzeltici Faaliyet Takip Formu

BGYS'nin işleyişi açısından kritik kontroller belirlenir ve BGYS Koordinatörü tarafından belirlenen ölçüm prosedür ve sıklığına uygun olarak etkinlikleri ölçülür.

Referanslar:

Risk Yönetimi Prosedürü

## Bilgi Güvenliği Amaçları ve Bu Amaçları Başarmak İçin Planlama

Kurumun Üst yönetimi, Bilgi Güvenliği yönetimi ile ilgili hedefleri belirlemekte ve hedefleri Etkinliği Ölçülecek Kontrol Listesi dokümante etmekte ve ilgili fonksiyon ve seviyelerde firma içinde iletilmesini sağlamaktadır.

Kurumun Bilgi Güvenliği hedefleri belirlenirken;

a) Bilgi Güvenliği politikası ile tutarlı olmasına

b) hedeflerin ölçülebilir olmasına,

d) geçerli koşulları dikkate almasına,

e) hedeflerin izlenmesine ve gerekli olduğu takdirde güncellenmesine dikkat edilmektedir.

Kurumun Bilgi Güvenliği hedeflerini gerçekleştirmek için her bir hedefle ilgili:

— ne yapılacağı,

— ne gibi kaynaklara ihtiyaç duyulacağı,

— kimin sorumlu olacağı,

— ne zaman tamamlanacağı ve

— sonuçların nasıl değerlendirileceği gibi bilgilerin Etkinliği Ölçülecek Kontrol Listesi bulunması sağlamaktadır.

**Referanslar:**

Hedef Takip Tablosu

## DESTEK

## Kaynaklar

Kurumun, BGYS’nin oluşturulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için ihtiyaç duyulan Personel, Yazılım, Ekipman, Bilgi ve Finans vb. kaynakları belirlemekte ve sağlamaktadır.

**Referanslar:**

-

## Yeterlilik

Kurumun **İnsan Kaynakları Prosedürleri** paralelinde;

Çalışan personelin performansını etkileyen yeterliliklerin neler olduğunu belirlemekte ve bu yeterlilikleri ilgili **Görev Tanımları**nda dokümante etmektedir.

Yeterlilik kriterlerine göre gerektiğinde, **Eğitim Prosedürü** paralelinde ihtiyaç duyulan eğitimler sağlanmakta, sağlanan eğitimlerin etkinliği değerlendirilmektedir.

**Referanslar:**

Eğitim Prosedürü

Görev Tanımları

Eğitim Kayıtları

## Farkındalık

Kurumun kontrolü altındaki çalışanlara, “**Eğitim Prosedürü”** paralelinde ihtiyaç duyulan eğitimleri sağlamakta, sağlanan eğitimlerin etkinliğini değerlendirilmekte paralelinde aşağıdaki konular hakkında farkındalık eğitimleri verilmekte ve kayıtları muhafaza edilmektedir: Farkındalık faaliyetleri en az aşağıdakiler içermektedir.

* Bilgi Güvenliği politikası,
* Gelişmiş Bilgi Güvenliği yönetim performansının faydaları dâhil BGYS’nin etkin olması için yapılacak katkılar,
* BGYS şartlarına uymamanın doğuracağı sonuçlar

**Referanslar:**

Eğitim Prosedürü

Görev Tanımları

Eğitim Kayıtları

## İletişim

Kurumun BGYS ile ilgili dahili ve harici iletişimlerini, **“Bilgi Teknolojileri Koordinatörlüğü İletişim Prosedürü”** ne göre yerine getirmektedir.

Bu anlamda prosedür

* Hangi konuların duyurulacağı,
* Ne zaman iletişime geçileceği,
* Kiminle iletişime geçileceği,
* Kimin İletişim Kuracağı ve
* İletişimin hangi süreçten etkileneceği

Konularında izlenecek yolu anlatmaktadır.

**Referanslar:**

Bilgi Teknolojileri Koordinatörlüğü İletişim Prosedürü

## Yazılı Bilgiler

## Genel

Kurumun BGYS Standardı paralelinde hazırlanması gereken dokümantasyonu, kurumun büyüklüğü, faaliyetlerimizin türü, proses, ürün ve hizmetleri, proseslerin ve etkileşimlerinin karmaşıklığı ve çalışanlarımızın vasıfları ölçüsünde hazırlamıştır, uygulamalara yönelik gereklilikleri yerine getirmektedir.

## Oluşturma ve Güncelleme

Kurumun bünyesinde herhangi bir doküman oluşturulurken ve/veya daha önceden oluşturulmuş bir doküman güncellenirken **“Doküman Yönetimi İşleyiş Prosedürü “**ndeki hususlara göre hareket edilir.

Her bir dokümana ait Başlık, Revizyon, Tarih, Hazırlayan, Onaylayan vb. hususlara dikkat edilir. Bilgi Güvenliği Yöneticisinin bilgisi olmadan doküman oluşturulamaz ve/veya yayından kaldırılamaz.

**Referanslar:**

Doküman Yönetimi İşleyiş Prosedürü

## Yazılı Bilgilerin Kontrolü

BGYS’de kullanılan tüm dokümanlar, kayıtlar ve raporlar sorumluları tarafından kontrol edilir, onaylanır ve dokümanın cinsine göre belirlenen konumlarda ve dosyalarında gizlilik derecelerine, bütünlük ve erişilebilirlik kıstaslarına uygun olarak saklanır.

Dokümanlarda bulunan bilgiler, BGYS içerisindeki faaliyetlerin göstergesidir ve yapacağımız geliştirme çalışmalarına da yol gösterici niteliktedir. Bu nedenle de dokümanların hazırlanması, kontrollü onayı, gözden geçirilmesi, sınıflandırılması, revizyonu, dağıtımı, sorumluları ve muhafazası konularını içeren prosedürler hazırlanmış ve uygulamaya sokulmuştur.

Kurumun oluşturulan ve kullanılan dokümanlar aşağıdaki gibi sınıflandırılabilir:

* Bilgi Güvenliği Politikaları,
* Bilgi Güvenliği Hedefleri,
* Varlık Envanteri ve Risk Değerlendirme Listesi,
* Prosedürler,
* Talimatlar,
* Formlar, el kitapları ve görev tanımlarıdır.

Bu madde kapsamında ISO 27001 Standardının bu sistemi uygulayanlardan istediği yazılı bir doküman oluşturulmuştur ve **“Doküman Yönetimi İşleyiş Prosedürü”** olarak yayımlanarak yürürlüğe girmiştir.

BGYS paralelinde yapılan uygulamaların delili niteliğindeki kayıtların saklanması, okunabilir olarak kalması ve korunması gibi hususların işlendiği **“Kayıtların Kontrolü Prosedürü”** de oluşturulmuş ve yürürlüğe konulmuştur.

**Referanslar:**

Doküman Yönetimi İşleyiş Prosedürü

Kayıtların Kontrolü Prosedürü

## İŞLETİM

## İşletimsel Planlama ve Kontrol

Kurumun, **Risk Yönetim Prosedürü** uygulamaları sonucu ortaya çıkan riskler ve fırsatları için kabul edilebilir seviyede olmayan riskler için de varlık envanteri ve risk değerlendirme tablosunda risk izleme sayfasında kontrol tedbirlerini belirlemekte, kontrolleri uygulamakta, kontrollerin etkinliğini “**Risk Yönetimi Prosedürü”** ile izlemektedir.

Kabul edilemez seviyede olan risklere yönelik alınan tedbirlerin planlandığı şekilde yerine getirildiğini gösteren dokümanlar “**Varlık Belirleme Sınıflandırma ve Etiketleme Talimatı” na** uygun olarak gizlilik içerisinde etiketlenir ve saklanır.

Kurumun, dış kaynaklı olarak yürütülen operasyonların kontrolünü de diğer operasyonel süreçlerde olduğu gibi kontrolü altında tutmakta, aynı yöntemle izlemektedir.

**Referanslar:**

Risk Yönetimi Prosedürü

Varlık Belirleme Sınıflandırma ve Etiketleme Talimatı

## Bilgi Güvenliği Risk Değerlendirme

Risk Değerlendirme; proseslerde, teknolojide, personel yetkinliğinde hiçbir değişiklik olmadı ise yılda en az bir defa tekrar gözden geçirilerek riskler güncellenmektedir. Kuruluşumuza yeni bir teknoloji alt yapısı kurulduğunda, yazılım değişikliklerinde, personel değişikliklerinde oluşabilecek bilgi güvenliği riskleri Varlık Envanteri ve Risk Değerlendirme Listesinde tekrar değerlendirilerek riskler için önleyici faaliyetler başlatılır.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

## Bilgi Güvenliği Risk İşleme

Kabul edilebilir risk seviyesinin üzerindeki tüm riskler için risk işleme planı “**Varlık Envanteri ve Risk Değerlendirme Listesi”** nde oluşturularak risk sorumluları tarafından süreç takip edilmektedir. Yeni değerlendirilen her kabul edilebilir risk seviyesinin üstündeki riskler için risk işleme planı oluşturularak riskler bertaraf edilmektedir.

Referanslar:

Varlık Envanteri ve Risk Değerlendirme Tablosu

## PERFORMANS DEĞERLENDİRME

## İzleme, Ölçme, Analiz ve Değerlendirme

Kurumun Etkinliği Ölçülecek Kontrollere ait bilgileri, “**Etkinliği Ölçülecek Kontrollerin Listesi”** adlı doküman aracılığı ile dokümante etmekte ve izlemektedir.

Bu dokümanda hangi ihtiyaçların izleneceği ve ölçüleceği, izleme, ölçme, analiz ve değerlendirme yöntemleri, izleme ve ölçmenin ne zaman yapılacağı, izleme ve ölçmeden elde edilen sonuçların ne zaman analiz edilip değerlendirileceği gibi hususlar detaylandırılmakta, izleme ve ölçmeye ilişkin kayıtlar muhafaza edilmektedir.

Kurumun BGYS performansı ve etkinliğini belirli periyotlarda yapılan Tatbikat ve Testler ve İç Tetkiklerle ölçmekte sonuçlarını YGG’lerde gözden geçirmektedir.

Kurumun, gerek **“Risk Yönetimi Prosedürü”** paralelinde ele alınan tehditler, gerekse **“DF Prosedürü”** paralelinde gelen önerileri dikkate almakta, bir uygunsuzluk meydana gelmeden önce olumsuz eğilim veya sonuçları değerlendirmekte, bu faaliyetler sonucu ortaya çıkan kayıtları saklamaktadır.

Performans izleme prosedüründe ele alınan konular şunlardır:

— Kurumun ihtiyaçlarına uygun performans metriklerinin oluşturulması,

— Kurumun Bilgi Güvenliği politikası, hedefleri ve amaçlarının ne kadarının karşılandığının izlenmesi,

— Kurumun öncelikli faaliyetlerini koruyan proses, prosedür ve fonksiyonların performansı,

— BGYS hedeflerine uygunluğun izlenmesi,

— BGYS uygunsuzluk, ramak kala, yanlış alarm ve güncel olaylar tarihsel kanıtların izlenmesi ve

— takip eden düzeltici tedbirleri kolaylaştırmak için izleme ve ölçme veri ve sonuçlarının kaydedilmesi.

**Referanslar:**

Risk Yönetimi Prosedürü

Düzeltici Faaliyet Prosedürü

Etkinliği Ölçülecek Kontrollerin Listesi

DF Kayıtları

## İç Tetkik

Kurumun, oluşturulan Bilgi Güvenliği Yönetim Sisteminin, şartları karşılayıp karşılamadığı hakkındaki bilgileri elde etmekte ve planlı aralıklarda “**İç Tetkik Prosedürü”** paralelinde iç denetim yapmaktadır:

İç Tetkiklerin planlanması, tetkikçilerin seçimi, tetkik sonuçlarının raporlanması ve gerekli hallerde Düzeltici faaliyetlerin açılmasında izlenecek yöntem “**İç Tetkik Prosedürü”** nde detaylandırılmaktadır.

İç denetim faaliyeti standardın gereksinimlerine ve yasal düzenlemelere, tanımlanan bilgi güvenliği gereksinimlerine uyum ve uygulanan kontrollerin etkinlik güvencesini sağlamak üzere yılda bir defa gerçekleştirilir. Denetimlerin planlanması ve gerçekleştirilmesindeki ve sonuçların raporlanması ve kayıtların tutulmasındaki sorumluluklar ve gereksinimler **"İç Tetkik Prosedürü”** nde tanımlanmaktadır.

İç denetçi havuzu yönetim sistemi denetimi için yetkin ve iç denetim ve/veya ISO27001 Uygulama / ISO27001 İç Denetim / ISO27001 Baş Tetkikçi eğitimlerinden bir veya daha fazlasını almış denetçilerden oluşturulmaktadır. Denetçiler kendi çalışmalarını denetlememektedirler.

**Referanslar:**

İç Tetkik Prosedürü

## Yönetimin Gözden Geçirilmesi

Kurumun Üst yönetimi, İSYS’ye sürekli uygunluğu, yeterliği ve etkinliği sağlamak için **YGG Prosedürü** paralelinde, planlı aralıklarla yönetim gözden geçirme toplantıları yapmaktadır.

Yönetimin gözden geçirmesinde aşağıdaki konular ele alınmaktadır:

a) daha önceki yönetim gözden geçirme faaliyetlerinin durumu,

b) Bilgi Güvenliği yönetim sistemi ile ilgili dâhili ve harici konularda meydana gelen değişiklikler,

c) aşağıdaki eğilimler dâhil bilgi güvenliği performansı hakkında bilgiler:

1) uygunsuzluklar ve düzeltici faaliyetler,

2) izleme ve ölçme değerlendirme sonuçları,

3) denetim sonuçları ve

4) Bilgi güvenliği amaçlarının yerine getirilmesi

d) ilgili taraflardan geri bildirimler

e) risk değerlendirme sonuçları ve risk işleme planının durumu

f) sürekli iyileştirme fırsatları.

**Referanslar:**

YGG Prosedürü

## İyileştirme

## Uygunsuzluk ve Düzeltici Faaliyet

Kurumun, BGYS kapsamında meydana gelen uygunsuzluklarda **Düzeltici Faaliyet Prosedürü** paralelinde işlem yapmaktadır.

Bir uygunsuzluk meydana geldiğinde Kurumun;

a) uygunsuzluğa karşı yapılacak faaliyetleri planlamakta:

b) uygunsuzluğun tekrarını önlemek ve ortadan kaldırmak için alınması gereken faaliyet ihtiyaçlarını değerlendirmekte,

c) ihtiyaç duyulan faaliyetleri uygulamakta,

d) alınan DF’lerin etkisini incelemekte,

e) gerekli olduğu takdirde Bilgi Güvenliği yönetim sisteminde değişiklik yapmak

f) gerçekleştirilen eylemlerin sonuçları ile

g) düzeltici faaliyetlerin sonuçlarını göz önünde bulundurmaktadır.

Kurumun bu faaliyet gereği ortaya çıkan DF kayıtlarını muhafaza etmektedir.

**Referanslar:**

Düzeltici Faaliyetler Prosedürü

## Sürekli İyileştirme

BGYS’nin sürekli iyileşmesini güvence altına alan ve sistemin sağlığı hakkında önemli bir gösterge olan düzeltici faaliyetlerin tespiti, uygulanması ve takibi ilgili prosedüre uygun olarak BGYS Koordinatörü koordinasyonunda gerçekleştirilir. Tüm personel düzeltici faaliyetlerin tespiti ve uygulanmasına farkındalık eğitimleri ve diğer duyurularla teşvik edilir.

Referanslar:

Düzeltici Faaliyetler Prosedürü

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EK-1 : BGYS İŞ AKIŞI | | | | |
| **HAZIRLIK**  **1.**  BGYS Ekibini Oluştur  **2.**  BGYS Kapsamını Belirle  **3.**  BGYS Yöneticisini Ata  **4.**  BGYS Proje Ekibini Kur  **5.**  Üst Yönetim Desteğini Al  **6.**  BGYS ve Bilgi Güvenliği Eğitimleri  **8.**  (Opsiyonel) Proforma BGYS Kurulum Bütçesini Hazırla  **7.**  Kapsam İçindeki Kritik İş Süreçlerini, Destekleyen Uygulamaları ve İlişkilerini İncele  **9.**  BGYS Politikasını Belirle / Gözden geçir  **10.**  Risk Değerlendirme Yaklaşımını ve Risk Kabul Kriterlerini Belirle  **11.**  ISO27002 Fark Analizi  **12.**  Teknik Zafiyet Analizi  **13.**  Bilgi Varlıklarını ve Sahiplerinin Belirle  **14.**  Risk Değerlendirmesini Yap ve Dokümante Et  **15.**  Risk İşleme Planını  Hazırla  **16.**  Risk İşleme Bütçesini Hazırla  **17.**  Risk İşleme Planı, Bütçesi ve Artık Risk İçin Yönetim Onayı Al  **18.**  Uygulanabilirlik Bildirgesini Hazırla  **19.**  Risk İşleme Planını Uygula  **Zorunlu Prosedürlerin Geliştirilmesi**  **20.**  Doküman ve Kayıt Yönetim Prosedürlerini Oluştur  **21.**  Olay Tespit, Veri Toplama ve Tepki Prosedürlerini Oluştur  **22.**  Kontrol Etkinliği Kriterlerini ve Ölçme Prosedürlerini Belirle  **23.**  İç Tetkik Prosedürünü Oluştur  **24.**  Bilgi Güvenliği Rol ve Sorumluluklarını Belirle  **25.**  Yönetim Gözetim Prosedürünü Oluştur  **26.**  Düzeltici Faaliyet Prosedürünü Oluştur  **27.**  Risk Analiz Prosedürünü Oluştur  **28.**  BGYS ve Bilgi Güvenliği Farkındalık Eğitim Prog. Oluştur  **29.**  BGYS Planlama Operasyon ve Kontrol  Prosedürünü Oluştur  **30.**  BGYS, Bilgi Güvenliği Eğitim ve Farkındalık Programını Uygula  **BGYS’nin İşletilmesi**  **31.**  Güvenlik Kontrollerini Uygulamaya Başla / Devam Et  **32.**  Sürekli İzleme Sürecine Başla / Devam Et  **33.**  Doküman Yönetimi, BSYG Kayıtlarının Kaydedilmesine (eğitim kayıtları dahil) Başla / Devam Et  **34.**  Risk Analizini Tazele  **35.**  BGYS İç Tetkikini  Gerçekleştir  **36.**  BGYS Yönetim Gözden Geçirme Faaliyetini Gerçekleştir  **37.**  Risk İşleme Planını Güncelle  **38.**  Bir Sonraki Dönem İçin BGYS Yatırım Harcama ve Eğitim Bütçesini Oluştur  **39.**  Belirlenen İyileştirmeleri, Düzeltici Faaliyetleri Uygula  **40.**  Düzeltici Faaliyetleri İçin İletişim Faaliyetini Gerçekleştir  **41.**  İyileştirmeler ve Düzeltici Faaliyetlerin Hedefine Ulaştığını Güvence Altına Almak İçin Takip Denetim Yap  Belgelendirme Denetimi | **PLANLAMA** | **UYGULAMA** | **KONTROL ETME** | **ÖNLEM ALMA** |
|  |  |  |  |  |

|  |
| --- |
| EK-2: BGYS STANDART MADDESİ İLE DOKÜMAN EŞLEŞTİRMESİ |

|  |  |  |
| --- | --- | --- |
| **ADIM NO** | **STANDART MADDESİ** | **İLGİLİ DOKÜMAN / KAYIT** |
|  | 4.1 | **-** |
|  | 4.2 | **-** |
|  | 4.3 | BGYS Kapsam Dokümanı |
|  | 4.4 | - |
|  | 5.1 | BGYS Ekibi Atama Yazısı |
|  | 5.2 | Bilgi Güvenliği Politika Dokümanı |
|  | 5.3 | BGYS Rol ve Sorumluluklar Dokümanı, BGYS Roller ve Sorumluluklar Dokümanı  BGYS Koordinatörü Atama Yazısı |
|  | 6.1 | Risk Yönetimi Prosedürü |
|  | 6.2 | BGYS Planlama Uygulama ve Kontrol Prosedürü, Etkinliği Ölçülecek Kontroller Listesi, Uygulanabilirlik Bildirgesi |
|  | 7.1 | - |
|  | 7.2 | İnsan Kaynakları Prosedürü  Eğitim Prosedürü |
|  | 7.3 | Eğitim Prosedürü, Yıllık Eğitim Planı, Eğitim Katılım Tutanakları |
|  | 7.4 | İletişim Prosedürü |
|  | 7.5 | Doküman Yönetimi İşleyiş Prosedürü, Kayıtların Kontrolü Prosedürü |
|  | 8.1 | Kontrollerin Etkinliğini Ölçme Prosedürü |
|  | 8.2, | Varlık Envanteri ve Risk Değerlendirme Listesi |
|  | 8.3 | Risk İşleme ve Artık Risk Onayı |
|  | 9.1 | Risk Yönetimi Prosedürü, DF Prosedürü, Etkinliği Ölçülecek Kontrollerin Listesi, DF Kayıtları |
|  | 9.2 | İç Tetkik Prosedürü, İç Tetkik Raporları |
|  | 9.3 | Yönetimin Gözden Geçirmesi Prosedürü, YGG Toplantı Tutanakları |
|  | 10.1 | Düzeltici Faaliyet Prosedürü, Olay İhlal Prosedürü, DF Formları |
|  | 10.2 | Düzeltici Faaliyetler Prosedürü |