1. Amaç

Bu dokümanının amacı Atatürk Üniversitesi Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönetim Sisteminin kapsam ve sınırlarını organizasyon, yerleşkeler ve altyapı bazında tanımlamaktır. Aynı zamanda bu doküman, kurumun bağlamını, genel yapısını, ilgili tarafların beklentilerini tanımlar.

BGYS Kapsamı, kurulacak sistemlerin değerlendirileceği ve uygun biçimde ele alınacağı alanı ifade eder. Onaylanmasından üst yönetim sorumludur. Kapsam ve sınır ifadelerindeki değişiklikler üst yönetim tarafından gözden geçirilir.

Teknolojik ve yasal değişiklikler ve iş fırsatları sonucu kurumun yapısı zaman içinde değişikliğe uğrayacağından bu doküman her yıl ve majör değişikliklerden sonra (bina, proses değişiklikleri vs.) gözden geçirilecek ve bu değişikliklerin etkilerini karşılamak için BGYS güncellenecektir.

2. Kapsam

Bu doküman, etkin bir yönetim sistemi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve sürekli iyileştirmek için Atatürk Üniversitesi Bilgi İşlem Daire Başkanlığı 'nın sistemlerin amaçlarını etkileyebilecek iç/dış hususları ve ilgili tarafların ihtiyaç ve beklentilerinin anlaşılması analizlerini kapsamaktadır.

3. Tanımlar

Kurum: Atatürk Üniversitesi Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

BGYS Amaçları: BGYS kurulması ile ulaşılmak istenen amaçlardır.

BGYS Hedefleri: BGYS amaçlarına ulaşmak için belirlenmiş olan hedeflerdir.

4. Kurumun ve Bağlamının Anlaşılması

Kurumumuz sağlamış olduğu hizmetlerde, yasal ve mevzuat şartlarının gerektirdiği düzeyde Bilgi Güvenliği faaliyetlerini yürütmeyi hedeflemektedir. Herhangi bir istenmeyen bilgi güvenliği riskleri için tanımlanan önceden belirlenen risklerin bertaraf edilmesi hedeflemektedir.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı

Bu anlamda kurumumuzun hizmet verme kapasitesini belirleyen, etkileyen iç ve dış konular; kamusal kaynaklardan edinilen, telefon, internet, elektrik, su, doğalgaz, kanalizasyon vb. konular, iç kaynaklardan sağlanan personel, tedarikçilerden alınan hizmetler, kurum alt yapısı ve teknolojik olanakları, finansal kaynaklı konular, güvenlik hizmetlerinden oluşmaktadır. Yukarıda belirtilen konular Kurumumuz bünyesinde BGYS'ni oluştururken, uygularken ve sürdürürken göz önünde bulundurulmakta ve sürekli gözden geçirilmektedir.

Bilgi Güvenliği İçeriği/Yapısı belirlenirken kurumumuz 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) Kurumumuzun risk potansiyeli göz önünde bulundurarak risk kriterleri belirlenmiş,

4) BGYS'nin amacı tanımlanmıştır.

4.1 İç ve Dış Hususların Belirlenmesi

Kurum'un iç ve dış hususlar ile olan ilişkileri, ilgili tarafların Kurumdan beklentileri değerlendirilmiştir ve BGYS'nin gerekliliği analiz edilmiştir. Bu doğrultuda; İç Hususlar, dış Hususlar ve yasal gereklilikler ifade edilmiştir.

Kurum'un Stratejik amaçları ve BGYS ile ilgili hedeflenen çıktılarına ulaşmasında etkisi olabilecek iç hususlar aşağıda verilmiştir.

HUSUS	ETKİSİ
Tecrübeli ve uygun eğitime sahip özveri ile çalışan personel varlığı	Kurum çalışanlarının belirli bir eğitim seviyesinde olması ve belirli şartları sağlayarak göreve başlamış olmaları bilgi güvenliği farkındalığının kısa sürede oluşmasına ve yaygınlaşmasına katkı sağlayacaktır.

İş gücünün istikrarı	Kurum çalışanlarının sirkülasyonunun fazla olması yönetim sistemine tüm çalışanların katılımına ve yayınlaşmasına olumsuz yönde etki oluşturmaktadır.
Yönetim İstikrarı	Yöneticilerin çok sık değişmemesi hem yönetim sistemine yönetimin desteğine hem de tüm çalışanların katılımına olumlu yönde etki oluşturmaktadır.
Kurum kültürü	Kurum bilgilerinin güvenliği konusunda bugüne kadar önemli bir olay yaşanmamasına rağmen bilgi güvenliği konusunda bir kültür oluşmuş olması, Kurumun bilgi güvenliğini ana hizmet kolları için gereklilik olarak görmesi BGYS'nin kurulması ve işletilmesi, sürekliliğinin sağlanması konularında olumlu etki oluşturmaktadır.
Yerleşke yapısı	Kurum Hizmetlerini tek yerleşkede hizmet vermemesi; BGYS'nin kurulması, bilgilerin güvenliğinin sağlanması, tüm çalışanların farkındalıklarının artırılması konularında olumsuz etki oluşturmaktadır.
Organizasyon yapısı	BGYS projesinin liderliğini yapan ve tüm Kuruma hizmet veren BGYS Komitesinin kurulması; BGYS'nin kurulması, sürekli iyileştirilmesi, konularında olumlu etki oluşturmaktadır.
Yeni personel istihdamı ile personel kaynağının güçlendirilmesi	Yeni personel istihdam edilmesi ile personeller arasında yedekliliğin sağlanması iç ve dış taraflara sunulan hizmetlerin ve Kurumsal süreçlerin sürekliliğine olumlu yönde katkı sağlanmaktadır.
Bilişim alt yapısının varlığı	Teknolojiye uygun Bilişim altyapısının varlığı BGYS'nin kurulması, bilgi güvenliğinin etkin şekilde sağlaması ve BGYS'nin sürekli iyileştirilmesi ne olumlu etki oluşturmaktadır.
Hizmet içi eğitimin yeterli olması	Yeterli hizmet içi eğitimlerin verilmesinden dolayı yeni istihdam edilen personelin hızlı bir şekilde hizmete kazandırılması BGYS'nin kurulmasında ve yaygınlaştırılmasında olumlu etki sağlamaktadır.

Hazırlayan	**Onaylayan**
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı

Verilen hizmetin aksamasının müşteriye etkisinin yüksel olması	Kurumun verdiği hizmet gereği hizmetin sürekliliğinin sağlanması ve takibinin önemi BGYS kurulmasında önemli etki sağlayacaktır.
Sunulan hizmetlerin iş adımlarının farklı programlardan takip ediliyor olması.	Kurumun verdiği hizmetlerin iş adımlarının farklı programlardan takip edilmesi BGYS nin kurulmasında olumlu etki sağlamıştır.
Mevcut bilişim kapasitesinin etkin kullanılması	Mevcut bilişim kapasitesinin etkin kullanılması BGYS kurulmasına olumlu yönde etki oluşturacaktır.

Kurumun BGYS ile ilgili hedeflenen çıktılarına ulaşmasında etkisi olabilecek dış hususlar aşağıda verilmiştir.

HUSUS	ETKİSİ
Altyapı hizmetleri	Kurumun altyapı ihtiyaçlarının karşılanması veya modernize edilmesi bilişim altyapının gelişimine katkıda bulunmaktadır. Bu katkı sayesinde bilişim faaliyetlerinin büyüyerek oluşması ihtiyaçlar ve gereksinimler ölçüsünde BGYS kurulmasına olumlu yönde etki oluşturacaktır.
Bilgisayar ve internet kullanımının artması	Ülkemizde internet ve bilgisayar kullanımının hızla artması nedeniyle müşterilerimizin işlemlerini online olarak yapma isteklerinin artması, Dijital ortamlardaki bilgilerin korunması ve erişim sürekliliği ihtiyacı da BGYS kurulmasına olumlu yönde etki oluşturacaktır.
Müşteriler ve Tedarikçiler	Müşteri ve tedarikçilerimizle sözleşmeler imzalayarak. Hem onların hem de kurumun gizlilik içeren belgelerinin sözleşmelerle garanti altına alınması. Kurumun itibarı ve kişilerin gizli bilgilerinin korunmasına destek olacaktır.
Sistemlerimizi kullanmak zorunda olan	Kurumun sunduğu hizmet gereği sahada sistemleri kullanan tedarikçilerin sayılarının fazla olması ve

tedarikçilerimizin çok olması	yönetilmesinin gerekliliği BGYS' nin kurulmasında olumlu etki sağlamıştır.

Kurumu doğrudan BGYS kurmaya zorlayan bir yasal düzenleme olmamakla birlikte mevcut olan bazı kanunlar, yönetmelikler, stratejiler, eylem planları vb. gerekliliklerini yerine getirmek için BGYS kurulması, sistematik bir şekilde yönetim sağlayacaktır.

*Kurumun BGYS ile ilgili hedeflenen çıktılarına ulaşmasında etkisi olabilecek yasal gereklilikler ve yükümlü olduğumuz diğer mevzuatların listesi Dış Kaynaklı Doküman Listesinde belirtilmiştir.

4.2 İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

Kurumun BGYS ile ilgili tarafları iç ve dış taraflar olmak üzere iki başlık altında ele alınmıştır. Belirlenen iç ve dış taraflar aşağıda verilmiştir.

4.2.1 İç Taraflar

a) Personel (Çalışanlar)

b) Yerine getirilecek politikalar, hedefler ve stratejiler,

c) Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),

d) Kurumun kültürü,

e) Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrıresmi),

f) Kurum tarafından uyarlanan standartlar, kılavuzlar, modeller ve Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.

4.2.2 Dış Taraflar

a) Gerçek-tüzel kişiler

b) Altyapı Sağlayıcı Şirketler (Telekomünikasyon, elektrik, su, doğalgaz vb.)

c) Yasa Koyucular

d) Yükleniciler (Temizlik, güvenlik, taşeronlar)

e) Tedarikçiler ve Müşteriler

Tarafların ihtiyaç ve beklentileri tabloda yer almaktadır.

İlgili Taraflar / **Beklentiler**	Personel (Çalışanlar)	Gerçek-tüzel kişiler	Altyapı Sağlayıcı Şirketler	Yasa Koyucular	Yükleniciler	Tedarikçiler ve
Personel özlük bilgilerinin güvenliğinin sağlanması	**X**					
Elektronik ortamda sunulan hizmetlerin sürekliliğinin sağlanması		**X**			**X**	
Kurum bilgilerinin güvenliğinin sağlanması				**X**	**X**	**X**
Vatandaş bilgilerinin güvenliğinin sağlanması		**X**		**X**		
Belge ve kayıtların güvenliğinin sağlanması		**X**		**X**		
Şirketlerin mali bilgilerinin güvenliğinin sağlanması				**X**	**X**	**X**
Veri transferi ortamlarının güvenliğinin sağlanması		**X**		**X**	**X**	**X**
Servisler arasındaki bağlantının güvenli bağlantı olmasının sağlanması				**X**	**X**	

Bilgi varlıklarının güvenliğinin sağlanması				**X**		
Bilgi güvenliğinin sağlanması için uyulması gereken politika ve prosedürlerin sağlanması	**X**	**X**	**X**	**X**	**X**	**X**

4.3 Kalite ve Bilgi Güvenliği Yönetim Sistemi Kapsamı

Atatürk Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yazılım geliştirme, donanım-teknik destek, ağ ve sistem yönetimi faaliyetlerinin yürütülmesi ve bu faaliyetler için kullanılan bilgi işlem faaliyetlerinin bilgi varlıkları ile bu varlıkları korumak amacıyla kullandıkları güvenlik önlemleri

Bilgi Güvenliği Yönetim Sistemi

Kurumumuz ISO 27001 standardı paralelinde ihtiyaç duyulan prosesler ve bunların etkileşimi dahil bir BGYS oluşturmuş, oluşturulan BGYS kurallarını uygulamakta, sürdürmekte ve sürekli olarak iyileştirmektedir.

5. Liderlik

Kurumumuz 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 yapmıştır.

Referanslar:

Yönetim Temsilcisi Atama Yazısı

Yönetim Taahhüdü

Kurum üst yönetimi, aşağıdakileri yerine getirerek BGYS ile ilgili liderlik ve taahhüdünü göstermektedir:

- Politika ve hedeflerin Bilgi Güvenliği yönetim sistemi için oluşturulmasını ve kurumumızın stratejik yönelimi ile uyumlu olmasını sağlamakta,

- Bilgi Güvenliği yönetim sistemi şartlarının kurumumızın 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, Bilgi Güvenliği Politikası belirleyerek, Bilgi Güvenliği Hedeflerinin İlgili Bilgi Güvenliği Planlarında belirlenmesini 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 getirmekte, temelde risk yaklaşımını göz önünde bulundurarak, iç tetkikleri ve YGG toplantılarını gerçekleştirmekte. sürekli iyileştirme taahhüdünü göstermektedir.

6. Planlama

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

7. Destek

7.1 Kaynaklar

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı

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

7.2 Farkındalık

Kurumumuz kontrolü altındaki çalışanlara, **Eğitim Prosedürü** paralelinde ihtiyaç duyulan eğitimleri sağlamakta, sağlanan eğitimlerin etkinliği değerlendirilmekte paralelinde aşağıdaki konular hakkında farkındalık eğitimleri verilmekte ve kayıtları muhafaza edilmektedir.

7.3 İletişim

Kurumumuz BGYS ile ilgili dahili ve harici iletişimlerini, **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.

7.4 Yazılı Bilgiler

Kurumumuz BGYS Standardı paralelinde hazırlanması gereken dokümantasyonu, Kurumumuzun büyüklüğü, faaliyetlerimizin türü, proses, ürün ve hizmetleri, proseslerin ve etkileşimlerinin karmaşıklığı ve çalışanlarımızın vasıfları ölçüsünde hazırlamıştır, uygulamalara yönelik gereklilikleri yerine getirmektedir.
Kurumumuz bünyesinde herhangi bir doküman oluşturulurken ve/veya daha önceden oluşturulmuş bir doküman güncellenirken Dokümanların Kontrolü Prosedürü 'ndeki hususlara göre hareket edilir.
Her bir dokümana ait Başlık, Revizyon, Tarih, Hazırlayan, Onaylayan vb. hususlara dikkat

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı

edilir. Bilgi Güvenliği Yöneticisinin bilgisi olmadan doküman oluşturulamaz ve/veya yayından kaldırılamaz.

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.

Kurumumuzda oluşturulan ve kullanılan dokümanlar aşağıdaki gibi sınıflandırılabilir:

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

Bu madde kapsamında ISO 27001 Standardının bu sistemi uygulayanlardan istediği yazılı bir doküman oluşturulmuştur ve **Dokümanların Kontrolü Prosedürü** olarak yayımlanarak yürürlüğe girmiştir.

8. İşletim

Kurumumuz, Risk Yönetim Prosedürü uygulamaları sonucu ortaya çıkan riskler ve fırsatları için kabul edilebilir seviyede olmayan riskler için de Bilgi Güvenliği Planları ile kontrol tedbirlerini belirlemekte, kontrolleri uygulamakta, kontrollerin etkinliğini Risk Yönetimi Prosedürü ile izlemektedir.

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

izlemektedir.

8.1 İşletimsel Planlama ve Kontrol

8.2 Bilgi Güvenliği Risk Değerlendirme

Risk Değerlendirme; proseslerde, teknolojide, personel yetkinliğinde hiçbir değişiklik olmadı ise yılda en az bir defa tekrar gözden geçirilerek riskler güncellenmektedir. Kurumumuza 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.

8.3 Bilgi Güvenliği Risk İşleme

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

9. Performans Değerlendirme

9.1 İzleme Ölçme Analiz ve Değerlendirme

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.

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

Kurumumuz, gerek Risk Yönetimi Prosedürü paralelinde ele alınan tehditler, gerekse DÖF 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.

9.2 İç Tetkik

Kurumumuz, 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.

9.3 YGG

Kurum 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,

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı

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.

10.İyileştirme

10.1 Uygunsuzluk ve Düzeltici Faaliyet

Kurum, BGYS kapsamında meydana gelen uygunsuzluklarda **Düzeltici ve Önleyici(DÖF) Faaliyet Prosedürü** paralelinde işlem yapmaktadır.

Bir uygunsuzluk meydana geldiğinde kurumumuz;

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 DÖF'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.

Kurumumuz bu faaliyet gereği ortaya çıkan DÖF kayıtlarını muhafaza etmektedir.

10.2 Sürekli İyileştirme

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

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Bilgi İşlem Daire Başkanı