

MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

İÇ TETKİK PROSEDÜRÜ

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 2 / 9

İçindekiler

1	Amaç	3
2	Kapsam.....	3
3	Sorumluluk	3
4	Tanımlamalar ve Kısaltmalar	3
5	İşlem Detayı	4
5.1	İç Tetkik Temel Kriterleri	4
5.2	Tetkik Planının Hazırlanması	4
5.3	İç Tetkik Hazırlıkları	5
5.4	İç Tetkikin Gerçekleşmesi	5
5.5	İç Tetkikin Raporlanması	7
5.6	Düzeltilici Faaliyetlerin İzlenmesi.....	8

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 3 / 9

1 Amaç

Bu doküman, Bilgi Güvenliği Yönetim Sisteminin, Politikalara, planlanmış süreçlere, prosedürlere ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardının şartlarına uygunluğunun gözden geçirilmesi, süreçlerin öz-değerlendirme prensibi doğrultusunda etkinliklerinin sorgulanması, birimler arasında bütünlüğün sağlanması, tetkikler aracılığıyla çalışanların yetkinliklerinin tespit edilmesi ve uygunsuzlukların giderilmesine yönelik yapılacak olan iç tetkik faaliyetlerinin tanımlanması amacıyla hazırlanmıştır.

2 Kapsam

Bu doküman, ISO 27001 Bilgi Güvenliği Kapsamı dokümanında belirtilen kapsamdaki tüm dokümanların, süreçlerin, birimlerin ve personelin tetkikini kapsamaktadır.

3 Sorumluluk

Görev Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
Birim BGYS Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/ Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 4 / 9

5 İşlem Detayı

5.1 İç Tetkik Temel Kriterleri

1. Kurum ISO 27001 faaliyetlerini yılda en az bir defa veya gerek duyulduğunda tetkik eder.
2. İç tetkik, kapsam dâhilindeki tüm birimlerde yapılır.
3. Tetkikler, iç tetkikçi yetkinliğine sahip tetkik ekibi tarafından yapılır. Tetkikler sırasında tetkikçiler ihtiyaç halinde uzman personelden destek alabilirler.
4. Tetkik süreleri ve tetkik ekibindeki tetkikçi sayısı, tetkik edilecek birimin büyüklüğü de dikkate alınarak BGYS Yöneticisi tarafından belirlenmelidir.
5. Tetkikçiler ISO 27001 BGYS temel eğitimini ve ISO/IEC 27001 İç Tetkik Eğitimini almış kişilerden seçilir.
6. Tetkikin tarafsızlığının sağlanması için tetkikçiler kendi birimlerini tetkik etmez.
7. Tetkikçiler tarafsız davranır.
8. Uygunsuzluklar gerçekçi ve/veya somut nedenlere dayandırılır. Tespit edilen uygunsuzluklar yapıcı olmalıdır.
9. İç tetkik sonrası elde edilen sonuçlar bu dokümanın 5.5 no'lu maddesine göre raporlanır.
10. 5.5 İç Tetkik'in Raporlanması maddesinde anlatıldığı şekilde kesinleşen bulgular için **DF Prosedürüne** uygun düzeltici faaliyet başlatılır.

5.2 Tetkik Planının Hazırlanması

1. BGYS Yöneticisi ilgili birim ile tetkik zamanı konusunda görüşme yaparak İç Tetkik Planını hazırlar.
2. Tetkik planında;
 - a. Tetkik edilecek birimler,
 - b. Tetkik tarihi ve süreleri,
 - c. Tetkiki gerçekleştirecek Tetkikçilerin isimleri bulunur.
3. Tetkik edilecek birimlerin organizasyonu, dokümanları ve süreçleri aşağıdaki şartlar dikkate alınarak “İç Tetkik Kontrol Listesi” oluşturulur veya güncellenir.
 - a. ISO 27001 şartları,
 - b. Önceki tetkiklerde tespit edilen uygunsuzlukların takibi,

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 5 / 9

- c. Tetkik edilecek birimlerle ilgili yasal mevzuat,
 - d. Tetkik ekibi tarafından ihtiyaç duyulabilecek diğer tetkik kriterleri.
4. BGYS Üst Yönetim Temsilcisi tarafından onaylanan iç tetkik planı tetkik edilecek birimlere en az 1 hafta önceden duyurulur.

5.3 İç Tetkik Hazırlıkları

1. BGYS Yöneticisi, tetkikler gerçekleştirilmeden önce tüm tetkik ekibini bir araya getirerek tetkik programı hakkında bilgilendirir. Bu değerlendirme sırasında, tetkik edilecek birime ilişkin;
 - a. Bilgi Güvenliği Politikası
 - b. BGYS dokümanları
 - c. BGYS Hedefleri
 - d. Mevcut ve önceki tetkikten sonra kapatılmış düzeltici faaliyetler
 - e. İç Tetkik Kontrol Listesi
2. Tetkikçiler, tetkik edilecek Birim Sorumluları ile tetkikin planlandığı haftadan önce temas kurar ve aşağıdaki işlemleri gerçekleştirir.
 - a. Tetkik Günü ile Açılış Toplantısının yeri ve saati karşılıklı olarak kararlaştırılır. Olağan dışı bir durum gerçekleşmesi halinde BGYS Yöneticisine bildirilerek tetkik haftasının değiştirilmesi talep edilir. Değişiklik BGYS Yöneticisi tarafından uygun görülürse “İç Tetkik Planı” revize edilir.
 - b. Tetkik günü tetkik edilecek süreç/birimle ilgili tüm faaliyetleri kapsayacak şekilde bilgi verebilecek asgari personelin bulunması gereği iletilir ve teyit edilir.

5.4 İç Tetkikin Gerçekleşmesi

1. Tetkik, daha önceden kararlaştırılan tarih, saat ve yerde açılış toplantısı ile başlar.
2. Açılış Toplantısı’na Tetkikçiler, BGYS Yöneticisi, İlgili Birim Yöneticileri ve Birim BGYS Sorumluları katılır. Açılış toplantısına gerektiğinde Birim BGYS Sorumluları ve/veya İlgili Birim Yöneticileri tarafından uygun görülen diğer personel de katılır.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 6 / 9

3. Açılış toplantısını BGYS Yöneticisi yönetir. Bu toplantılar çok özel bir durum olmadığı takdirde 15 dakikayı geçmeyecek şekilde planlanır. BGYS Yöneticisi Açılış Toplantısı’nda aşağıdaki konuları açıklar:
- Tetkikin amacı ve kapsamı
 - Tetkikçi ve tetkik edilenlerin tanışması
 - Bulunabilecek uygunsuzluklara ait izlenecek yöntemler
 - İç tetkiklerin örneklemeye dönük yaklaşımı
 - Tetkik sırasında tetkikçilere eşlik edecek kılavuzların atanması
 - Tetkikçiler arasında yapılan iş bölümü ve planlama
 - BGYS Sorumlusu tarafından Tetkikçinin bilgilendirilmesi gereken kural ve düzenlemeler
 - Yemek araları ve diğer araların planlanması
 - Kapanış Toplantısı’nın planlanması
4. İç tetkik, hazırlanan tetkik planına göre belirlenmiş tarih ve saatler arasında tetkik edilecek birim ziyaret edilerek yapılır.
5. Tetkikçiler yapılan iş bölümüne göre, “**İç Tetkik Kontrol Listesi**” ve diğer dokümanları kullanarak tetkiki gerçekleştirirler. Tetkik esnasında konuyla ilgili sorular sorar, gözlem yapar, doküman ve kayıtları incelerler. Tetkik esnasında “**İç Tetkik Kontrol Listesi**” nde mevcut olmayan sorular sorulabilir. Bu durumda sorular listeye ilave edilir.
6. Tetkik esnasında tespit edilen herhangi bir uygunsuzluk tarafsız ve somut delillerle, tetkik edilen personele açıklanır.
7. “**İç Tetkik Kontrol Listesi**” nde yer alan soruların değerlendirmesi “Uygun, Uygun Değil veya Gözlem” olarak formun üzerinde işaretlenir ve tetkik ile ilgili olumlu ve olumsuz bulgular, dokümanlar, kayıtlar, notlar ve yorumlar formun üzerinde belirtilir.
8. Tetkik yapılan faaliyetle ilgili dokümantasyonun yeterli olması, faaliyetlerin dokümanlarda belirtildiği şekilde uygulanması ve belirlenmiş politika ve hedeflere ulaşılmasında etkin olması durumunda “Uygun” işaretlenir.
9. Sorulara yeterli cevap alınamayan, doküman ve kayıtlarla doğrulanamayan, varlığı kanıtlanamayan cevaplar bulunan ve uygulama sonuçlarının etkin olmadığı gözlenen her konu ile ilgili “Uygun Değil” işaretlenir.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 7 / 9

10. Sorulara yeterli cevap alınamayan, uygulaması bulunan ancak doküman ve kayıtlarla kısmen doğrulanabilen konu ile ilgili “Gözlem” işaretlenir ve “**İç Tetkik Raporu**” nda gözlem yazılır.
11. “Uygun Değil” veya “Gözlem” kısmının işaretlenmesi durumunda öngörülen Düzeltici Faaliyetler not olarak “**İç Tetkik Kontrol Listesi**” nde belirtilir.
12. Tetkikçiler, tetkik sırasında herhangi bir problem çıktığı takdirde (bulgulara itiraz, tartışma, tetkiki aksatacak herhangi bir şey) BGYS Yöneticisini haberdar ederler.

5.5 İç Tetkikin Raporlanması

1. Tetkik tamamlandıktan sonra konuyla ilgili birim sorumlularının, BGYS Yöneticisinin ve BGYS Sorumlularının katılımı ile aşağıdaki gündeme göre bir kapanış toplantısı gerçekleştirilir;
 - a. Tetkikin amacı ve kapsamı
 - b. İç tetkikin örneklemeye dönük yaklaşımı
 - c. Tetkik sonucu bulguların sunulması
 - d. Açıklama
 - e. Düzeltici faaliyet önerileri
 - f. Toplantının kapatılması
2. Kapanış toplantısı sırasında, tetkik sonuçları ile ilgili olarak ilgili birim sorumlusu ile mutabakata varılması esastır. Bu nedenle tetkikçi, uygunsuzluklar ve iyileştirme olanakları hakkında, birim sorumlularına somut delillerini sunar ve bulguları teyit eder.
3. Üzerinde mutabakat sağlanan her bir uygunsuzluk için Düzeltici Faaliyet (DF) başlatılır. Uygunsuzlukların/İyileştirici faaliyetlerin giderilmesi için gerekli çalışmalar yapılarak “**Düzeltici ve İyileştirici Faaliyet Prosedürü**” ne göre sonuçlandırılması sağlanır.
4. Mutabakat sağlanamayan uygunsuzluklar için karar Üst Yönetim Temsilcisi tarafından verilir.
5. İç Tetkik Raporu, Tetkikçiler tarafından BGYS Yöneticisine verilir.
6. Kapanış toplantısı gerçekleştirildikten sonra en geç 1 hafta içerisinde “İç Tetkik Raporu” hazırlanır. Bu raporda; bulunan uygunsuzluklar, düzeltici faaliyetler ve terminleri açık bir biçimde tanımlanır. Bulunan uygunsuzluklarla ilgili kayıtlar (gerekliyse) raporun ekine konulur.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 8 / 9

7. BGYS Yöneticisi gelen iç tetkik raporunun tamamını ya da ilgili kısımlarını Birim BGYS Sorumluları ve/veya ilgili birim yöneticileri ile paylaşır.
8. İç tetkik raporu yönetim gözden geçirme toplantılarında BGYS Yöneticisi tarafından üst yönetime sunulur.

5.6 Düzeltici Faaliyetlerin İzlenmesi

1. Belirlenen düzeltici ve iyileştirici faaliyetlerin planlanan zamanlarda yerine getirilmesini takip etmek BGYS Yöneticisi sorumluluğundadır.
2. Gerek görülürse uygunsuzluğu bulan Tetkikçiler Düzeltici Faaliyetler için takip tetkiki yapar veya BGYS Yöneticisi, uygunsuzluğun önem derecesine göre takibini bir sonraki planlı tetkik dönemine bırakabilir. Böyle bir durumda takip, bir sonraki tetkik sırasında, o tetkikte görev alacak tetkikçiler tarafından gerçekleştirilir.
3. Takip tetkikinin sonucuna göre uygunsuzluklar giderilmişse DF kapatılır veya uygunsuzlukların giderilmesi için ek süre verilir. Ek süre sonunda da uygunsuzluklar giderilmemişse yeni bir DF isteğinde bulunulur.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	İÇ TETKİK PROSEDÜRÜ	Doküman No	PR.04
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 9 / 9

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	