Revizyon Takip Tablosu

Versiyon	Tarih	Revizyonu Yapan	Değişiklik Notu

Dağıtım Takip Tablosu

Adı Soyadı	Tarih	Ünvan

Hazırlayan	Kontrol eden	Onaylayan

İçindekiler

Giriş

Tanımlar

Politika, Prosedür ve Talimat dokümanlarında geçen terim ve kısaltmalar, ek olarak tanımlar tablosunda belirtilmiştir.

1. Amaç

Bilgi Güvenliği El Kitabı'nın amacı 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.

2. Kapsam

Bilgi Güvenliği El Kitabı, ISO 27001 Standardı olan Bilgi Güvenliği Yönetim Sistemi'nin organizasyon ve faaliyetlerine uygun biçimde uygulanma biçimini, yönetim sisteminin uyarlanması ve işletimi sırasında uygulanan politika, prosedür ve kayıtları kapsamaktadır.

3. Sorumluluklar

Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Yönetim Temsilcisi sorumludur. BGYS Komite Üyeleri ve Yönetim Temsilcisi Üst Yönetim tarafından atanmıştır. Kapsam içindeki departmanlardan BGYS Komite üyeleri belirlenmiştir. BGYS komite üyesi olarak isim bazında atamaları yapılmıştır.

4. Kuruluşun Bağlamı

4.1. Kuruluşun bağlamının anlaşılması

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir.

İç Bağlamı;

SBÜ yönetimi bünyesinde bulunan kapsam dâhilindeki departmanlar. BGYS Politikaları, Yıllık BGYS hedefleri, Kaynaklar (örneğin; zaman, kişiler, süreçler, sistemler ve teknolojiler), BGYS kurulması, işletilmesi ve sürdürülmesi için yönetim tarafından atanan Yönetim Temsilcisi ve BGYS ekibi, İç paydaşlarla ilişkiler, onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.

Dış Bağlamı;

Yasal mevzuatlar, Ulusal Siber Güvenlik Eylem Planı ve Yükseköğretim Kurulunun talimatları, Teknolojik değişimler, başka kurumların Bilgi Güvenliği ihlal olaylarından ders çıkarma, Çevresel olaylar ve doğal afetler, Siber saldırılar, Kurum itibarı.

4.2. İlgili tarafların ihtiyaç beklentilerinin anlaşılması

İlgili Taraflar
Çalışanlar, Üst Yönetim, Akademisyenler, Öğrenciler, Tedarikçiler ve İş Ortakları, Düzenleyici ve Denetleyici Kurumlar, Otoriteler, Dış Denetçiler.

İlgili Taraflar ve Beklentileri

İlgili Taraflar	İhtiyaç ve Beklentiler
Çalışanlar *(İdari ve Destek Personeli)*	- Kendilerine teslim edilen bilgi varlıklarının (bilgisayar, yazılım, e-posta) güvenli kullanım ilkelerinin net olması. - BGYS politikaları, prosedürler ve KVKK konusunda düzenli farkındalık eğitimleri alabilmek. - Özlük, maaş ve sağlık verilerinin gizliliğinin ve güvenliğinin korunması. - İntranet ve kurumsal sistemlere güvenli, yetkisi dahilinde ve kesintisiz erişim.
Üst Yönetim *(Rektörlük, Mütevelli Heyeti / Senato)*	- Üniversitenin itibarının, vizyonunun ve kurumsal verilerinin korunması. - BGYS risklerinin (yasal cezalar, veri sızıntıları, hizmet kesintileri) minimuma indirilmesi. - BGYS'nin stratejik hedeflerle uyumlu çalışması ve mevzuata (KVKK, DDO Rehberi, YÖK vb.) %100 Uyum. - İç/dış denetim sonuçları ve BGYS performansı hakkında düzenli YGG (Yönetimin Gözden Geçirmesi) raporlaması.
Akademisyenler *(Öğretim Üyeleri ve Elemanları)*	- Araştırma verileri, telif hakları, proje çıktıları ve akademik çalışmaların gizliliği ve bütünlüğünün korunması.

	- Araştırma laboratuvarları, veri tabanları ve akademik sistemlere güvenli ve kesintisiz erişim. - Öğrenci not girdileri ve değerlendirme sistemlerinde yetkisiz erişimlerin engellenmesi. - Uzaktan eğitim ve dijital içeriklerin yetkisiz kopyalanmaya/dağıtıma karşı korunması.
Tedarikçiler ve İş Ortakları *(Yazılım, Donanım, Güvenlik, Yemek, Temizlik vb.)*	- Sözleşmelerde yer alan Bilgi Güvenliği ve KVKK taahhütlerinin net ve uygulanabilir olması. - Kendilerine verilen fiziksel/mantıksal erişim yetkilerinin sınırlarının açıkça çizilmesi. - Tedarikçi bilgilerinin ve ticari sırların gizli tutulması. - Ödemelerin ve hizmet süreçlerinin güvenli altyapılar üzerinden yürütülmesi.
Öğrenciler *(Önlisans, Lisans, Lisansüstü, Mezunlar)*	- Öğrenci Bilgi Sistemi (ÖBS), e-posta ve Wi-Fi hizmetlerinin kesintisiz ve güvenli olması. - Kişisel verilerinin (kimlik, iletişim, sınav/not bilgileri, disiplin/sağlık kayıtları) KVKK'ya uygun korunması. - Sınav ve mezuniyet süreçlerinde veri bütünlüğünün korunması (notların değiştirilememesi). - Hizmet sağlayıcılarla yapılan öğrenci sözleşmelerinde bilgi güvenliği şartlarına uyulması.
Düzenleyici ve Denetleyici Kurumlar (KVKK, YÖK, YÖKAK, Rekabet Kurumu, Cumhurbaşkanlığı DDO)	➢ **KVKK (Kişisel Verileri Koruma Kurumu):** - Kişisel verilerin ve özel nitelikli kişisel verilerin hukuka uygun işlenmesi, aktarılması ve imhası. - VERBİS kaydının güncel tutulması. - Olası bir veri ihlali durumunda Kurum'a (en geç 72 saat içinde) ve ilgili kişilere bildirim yapılması. - Veri güvenliğine ilişkin idari ve teknik tedbirlerin (erişim yetkileri, şifreleme,

	sızma testleri, loglama vb.) eksiksiz uygulanması. ➢ **YÖK & YÖKAK:** - Eğitim-öğretim, öğrenci ve akademik süreçlere ait verilerin bütünlüğü, doğruluğu ve gizliliğinin korunması. - İstenen resmi rapor, istatistik ve belgelerin zamanında ve doğru teslim edilmesi. ➢ **Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO):** - Bilgi ve İletişim Güvenliği Rehberi kapsamında kurum veri seviyelendirmesinin yapılması ve rehberdeki güvenlik tedbirlerine uyum sağlanması. ➢ **Rekabet Kurumu:** - Kurumsal/ticari sırların ve hassas verilerin korunması, mevzuata uygun hareket edilmesi.
Otoriteler *(BTK, Siber Suçlar / Emniyet, Bakanlıklar, Belediyeler, İtfaiye)*	➢ **BTK ve Emniyet Genel Müdürlüğü (Siber Suçlarla Mücadele):** - **5651 Sayılı Kanun Uyarınca:** İnternet toplu kullanım sağlayıcı olarak kullanıcı trafik kayıtlarının (IP/DHCP logları) zaman damgalı ve değiştirilemez şekilde saklanması. - Siber olay adli incelemelerinde makamlardan gelen bilgi/belge taleplerine zamanında yanıt verilmesi ve Kurumsal SOME (Siber Olaylara Müdahale Ekibi) süreçlerinin işletilmesi. ➢ **İçişleri Bakanlığı / Belediyeler / İtfaiye:** - Veri merkezi ve sistem odalarında fiziksel güvenlik, iklimlendirme, yangın söndürme ve gaz algılama standartlarına (yönetmelik ve ruhsat şartlarına) uyum sağlanması. - İş Sürekliliği ve Felaket Kurtarma Planları kapsamında fiziksel çevre güvenliğinin korunması. ➢ **Genel Uyumluluk:**

	- Kurumun tabi olduğu tüm yasa, yönetmelik, lisans ve taahhütnamelere uygun hareket edilmesi, olası bir uygunsuzluk durumunda ilgili otoritelerin bilgilendirilmesi.
Dış Denetçiler *(ISO 27001 Belgelendirme Denetçileri, Sayıştay, Bağımsız Denetçiler)*	- BGYS dokümantasyonunun (Politikalar, Prosedürler, Görev Tanımları, Risk Analizleri) güncel ve erişilebilir olması. - Denetim kanıtlarının (loglar, eğitim katılım formları, sızma testi raporları, bakım sözleşmeleri) eksiksiz sunulabilmesi. - İç denetim ve DÖF (Düzeltici Önleyici Faaliyet) mekanizmasının efektif çalıştığının gösterilmesi.

4.3. Bilgi Güvenliği Yönetim Sisteminin Kapsamı

Sağlık Bilimleri Üniversitesi Bilgi İşlem Daire Başkanlığı Yetki ve Görev Alanında Bulunan Bilişim Sistemlerinin, Network ve Sistem Altyapılarının Planlanması, Kurulumları, Yönetilmesi ve Gerekli Donanım ve Yazılımların Satın Alınması, Kurulu Sistemlerin ve Bilgilerin Güvenliğinin Sağlanması, İletişim ve İnternet Altyapısı Yeniliklerinin Uygulanması olarak belirlenmiştir.

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.

1. BGYS faaliyetlerinde sponsorluk yapılması,
2. BGYS politika ve amaçlarının kurumun strateji ve hedefleri ile uygun olmasının gözetilmesi,
3. BGYS gereksinimlerinin organizasyon süreçlerine entegre olmasının sağlanması,
4. BGYS için gerekli kaynağın ayrılması,
5. BGYS'den beklenen çıktıların alınmasının sağlanması,
6. Personellerin BGYS'nin etkinliğine katkıda bulunması için onlara destek olunması ve yönlendirilmesi,
7. Sürekli iyileştirmenin desteklenmesi,
8. Kendi liderliklerini pekiştirmek için kendi sorumlulukları dahilinde ilgili yönetim rollerinin desteklenmesi.

5.2. Politika

İlgili Dokuman
Bilgi Güvenliği Politikası

5.3. Kurumsal Roller Sorumluluk ve Yetkiler

Üst yönetim tarafından BGYS sorumlulukları atanmış ve tanımlanmıştır.

İlgili Dokuman
BGYS Ekibi ve BGYS Yönetim Temsilcisi Atama Yazısı
Organizasyon Şeması

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 Analizi ve Değerlendirme Listesi'nde yapmaktadır.

6.1. Bilgi Güvenliği Risk Değerlendirmesi

Bilgi güvenliği risk değerlendirme süreci tanımlanmıştır.

İlgili Dokuman
Risk Yönetim Prosedürü

6.2. Bilgi Güvenliği Amaçları ve Bu Amaçları Gerçekleştirmek İçin Planlama

Bilgi güvenliği hedefleri ulaşabilmek adına Yönetim Gözden Geçirme (YGG) Prosedürü kapsamında belirtilen sayı ve sürede toplantılar gerçekleştirilir.

İlgili Dokuman
BGYS Amaç ve Hedef Planı

7. Destek

7.1. Kaynaklar

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

7.2. Yeterlilik

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

İlgili Dokuman

Görev Tanımları
Yıllık Eğitim Planı
Oryantasyon Formu
Eğitim Katılım Formu

7.3. Farkındalık

Kurumumuzun Personelleri tarafından görev tanımlarında belirtilmiş olan işlemlerin gerçekleşmesi ve daha güvenli ve performanslı süreçlerin ilerlenmesi amacıyla eğitim planlaması yapılır ve eğitimler gerçekleştirilir.

İlgili Dokuman

Görev Tanımları
Yıllık Eğitim Planı
Oryantasyon Formu
Eğitim Katılım Formu

7.4. İletişim

Kurumumuzun dahili ve harici iletişim kaynaklarını yetkililerce onaylanmış kişiler üzerinden sağlamaktadır.

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

İlgili Dokuman

Otoriteler ve İlgi Grupları İletişim Listesi

7.5. 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 ve Kayıtların Kontrolü 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.

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 Doküman ve Kayıt Kontrolü Prosedürü olarak yayımlanarak yürürlüğe girmiştir.

İlgili Dokuman
Doküman ve Kayıt Kontrolü Prosedürü

8. İşletim

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

Kurumumuz bünyesindeki bilişim cihazlarının amaçları doğrultusunda kullanımı hakkında kuralları tanımlamaktır.

8.1. İşletimsel Planlama ve Kontrol

Kurumumuz bilgi güvenliği şartlarını karşılamak ve madde 6.1 de belirlenen faaliyetleri gerçekleştirmek için gerekli olan süreçleri planlamakta, uygulamakta ve kontrol etmektedir. Kuruluşumuz Bilgi Güvenliği Amaçlarına ulaşabilmek için planları uygulamaktadır.

Yazılı bilgiler Doküman ve Kayıtların Kontrolü Prosedürü'ne göre saklanmaktadır. Planlanan değişiklikler kontrol edilmekte istenmeyen değişikliklerin kötü etkileri için anında aksiyon oluşturulmaktadır.

İlgili Dokümanlar
Doküman ve Kayıtların Kontrolü Prosedürü

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.

İlgili Dokuman
Yönetim Gözden Geçirme (YGG) Prosedürü

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 Dokumanlar
İç Denetim Prosedürü

9.3. Yönetimin gözden geçirmesi

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 dokumante edilmekte ve kayıtları tutulup saklanmaktadır.

9.4. Gözden Geçirme Girdisi

Yönetimin gözden geçirmesinin girdileri aşağıdakileri içermektedir:

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

İlgili Dokumanlar
Yönetim Gözden Geçirme Prosedürü

10. İyileştirme

10.1. Uygunsuzluk Düzeltici Faaliyet

Kuruluş tekrarları engellemek için, BGYS gereksinimleriyle uygunsuzlukların nedenlerini gidermek üzere önlemler almaktadır. Düzeltici faaliyet için dokumante edilmiş prosedür (İç Denetim Prosedürü) aşağıdaki gereksinimleri tanımlamaktadır.

1. Uygunsuzlukları tanımlama,
2. Uygunsuzlukların nedenlerini belirleme,
3. Uygunsuzlukların tekrarlanmamasını sağlamak için ihtiyaç duyulan faaliyetleri değerlendirme,
4. Gereken düzeltici faaliyetleri belirleme ve gerçekleştirme,
5. Gerçekleştirilen faaliyetlerin sonuçlarını kaydetme
6. Gerçekleştirilen düzeltici faaliyetleri gözden geçirme.

İlgili Dokumanlar

İç Denetim 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.