BGYS-KEK-01

EL KİTABI

İÇİNDEKİLER

1. Amaç

Bu el kitabının hazırlanmasında amaç Sivas Cumhuriyet Üniversitesi'nin yürürlükteki bilgi güvenliği yönetim sistemini açıklamak, sistemin uygulanmasından sorumlu yönetici personelin yetki ve sorumluluklarını tanımlamak, bilgi güvenliği sistemini oluşturan tüm faaliyetler için genel prosedürler tanıtmaktır.

2. Kapsam

Bu doküman, Kapsam Analizi Dokümanında belirtilen birimlerde gerçekleştirilecek tetkiklerin öncesi teknik açıklık kontrollerini kapsar.

3. Revizyon Kayıtları ve Doküman Onayları

Revizyon No	Tarih	Revizyon Nedeni	Revizyon Sayfa No	Revize Edilen Bölüm

3.1. Doküman Onayları

Hazırlayan	Kontrol Eden	Onaylayan
Aykut KAYA **BGYS Ekip Üyesi**	**Yusuf EĞRİ** **BGYS Yöneticisi**	**Ayhan ÖZDEMİR** **BGYS Üst Yönetim Temsilcisi**

4. Tanımlamalar ve Kısaltmalar

Kısaltmalar ve tanımlamalar kılavuzunda belirtilmiştir.

5. Uygulama

5.1. Bilgi Güvenliği Politikası

Misyonu, İnsanı temel alan bir eğitim anlayışı dairesinde, beynelmilel faydalı bilgiye ulaşmayı ve üretmeyi ilke edinen, çevresel, toplumsal ve tarihsel milli ve manevi değerlere sahip ve saygılı, bölgenin ve ülkenin ekonomik, sosyal ve kültürel gelişimine katkı sunan, ulusal ve uluslararası rekabet koşullarında işbirliği ve araştırmalara açık, araştıran, çözümleyen evrensel öğrenci ve akademisyenler yetiştirmektir. Bu misyona uygun olarak Sivas ölçeğinde temel görevler üstlenerek bilim ve eğitim merkezi olmak, bu sayede bölgenin ve ülkemizin geleceği ve kalkınmasına katkı sağlamaktır

Kurumumuzda yasal uyumluluklar çerçevesinde gerektiği kadar bilme prensibine uygun erişim kontrolleri, gelişen teknolojiye uygun güvenlik önlemleri alınır. Bilgi güvenliği tehditleri göz önünde bulundurularak kuruluş bilgi varlıkları ve hizmetleri açısından riskler ve önlemler arasında uygun bir denge sağlayan bilgi güvenliği risk yönetimi sistemi uygular. Bu çerçevede bilgi güvenliği amaçlarımız;

1. Bilişim sistemlerinin yönetilmesinde bilgi güvenliği ve iş standardizasyonunun sağlanması
2. Kurumda işlenen verilerin gizlilik, bütünlük ve erişilebilirliğinin en üst seviyeye çıkartılması
3. Yasal gereksinimlere ve sözleşmelere uyumun sağlanması

Üst Yönetim olarak, belirlenen bilgi güvenliği amaçlarını gerçekleştirmek ve TS ISO/IEC 27001'de belirtilen gereksinimleri yerine getirecek şekilde tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağımızı ve sistemin verimli şekilde çalışması için gerekli olan kaynakların tahsis edileceğimizi, etkinliğini değerlendireceğimizi, sürekli iyileştireceğimizi ve bunun tüm ilgili taraflarca anlaşılmasını sağlayacağımızı taahhüt ederiz.

5.2. Kalite Hedefleri

Kurum, bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğini BGYS yöneticisinin koordinasyonunda BGYS ekibi ile "Ölçme ve Değerlendirme Listesi" aracılığı ile en az yılda bir kez ölçer. Yapılan ölçüm sonuçları YGG toplantılarında üst yönetime Üst Yönetim Temsilcisi tarafından sunulur. Ölçme ve değerlendirme listesi oluşturulurken bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere;

1. Neyin izlenmesi ve ölçülmesinin gerekli olduğu,
2. Uygun izleme, ölçme, analiz ve değerlendirme yöntemleri belirlenir.

İzleme ve ölçmede aşağıdaki başlıklar göz önünde bulundurulur:

1. İzleme ve ölçmenin ne zaman yapılacağı,
2. İzlemeyi ve ölçmeyi kimin yapacağı,
3. İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği,
4. Bu sonuçları kimin analiz edeceği ve değerlendireceği belirlenir.

5.3. Yönetim Sistemi İle İlgili İç ve Dış Hususlar

İç Hususlar

1. Kurumun destekleyici hizmet süreçlerinin bilişim sistemleri etkisinde olması
2. Kurum bilgi teknolojileri biriminin uzun süreli aynı personelin çalışarak bağlılıklarının olması
3. Kurum bilişim altyapısının genel yeterlilikleri sağlayabilecek olması.
4. Bilişim sistemlerinin yürütüldüğü birim bünyesinde personel sayısının yetersiz olması
5. Bilişim sistemlerinin yürütüldüğü birim dışında bilgi güvenliği yetkinliği ve farkındalığı olan personel sayısının az olması
6. Kurumdaki bilgi teknoloji faaliyetlerinin tek merkezden yönetiliyor olması

Dış Hususlar

1. Siber güvenlik tehditlerinin artması
2. Yasal gereksinimlerden doğan bilgi güvenliği yönetim sistemi gereksinimi temrin tarihlerinin yaklaşmış olması
3. Bilişim güvenliğini etkileyen yasal gereksinimlerin var olması (Yükseköğretim Kurulu Başkanlığı Yazısı, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kişisel Verilerin Korunması Kanunu)
4. Kurum teknolojik iyileştirmelerin döviz artışından etkilenmesi
5. Kurum lokasyonunda bilgi teknolojileri hizmeti veren tedarikçi firma sayısı azlığı.

5.4. Yönetim Sistemi İle İlgili Taraflar ve Bunların Şartları

Kurumun Yönetim Sistemi gereksinimler belirlenirken ilgili taraflar ve yasal gereksinimler belirlenir. Aşağıda Yönetim Sistemi ile ilgili taraflar belirtilmiştir;

İlgili Taraflar / **Beklentiler**	**Kurum Çalışanı**	**Öğrenciler**	**Hastane**	**Dış Tedarikçiler**	**Üniversiteler**	**İl Göç İaresi**	**Emniyet**	**Savcılık**	**Erasmus**	**Valilik**	**Bağlı Meslek Yüksek Okullar**	**İlgili otoriteler**	**Kurum Diğer Birimleri**	**Sivil Toplum Kuruluşları**	**Üst Yönetim**
Kurumsal Bilgi Güvenliği Yönetim Sistemine uyulması												□			
Kişisel Verilerin Güvenliğinin sağlanması	□	□	□											□	
Ticari Bilgilerinin				□											

Güvenliğinin Sağlanması														
İş süreçlerinde kullanılan verilerin gizliliğinin bütünlüğünün ve erişilebilirliğin in sağlanması					□	□	□	□	□	□	□		□	□
Üniversite'de BGYS'nin sürekli iyileştirilerek devam ettirilmesi	□											□		□

5.5. Yönetim Sisteminin

Kurum bünyesinde kullanılan, üretilen veya işlenen her türlü bilgi ve bilgi işleme ortamının güvenliğinin sağlanması ve sistematik bir şekilde sürdürülebilmesi için, TS ISO/IEC 27001 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler standardına uygun olarak bir Bilgi Güvenliği Yönetim Sistemi kurulmasına karar verilmiştir. Yukarıda belirtilen analizler sonucunda BGYS kapsamı;

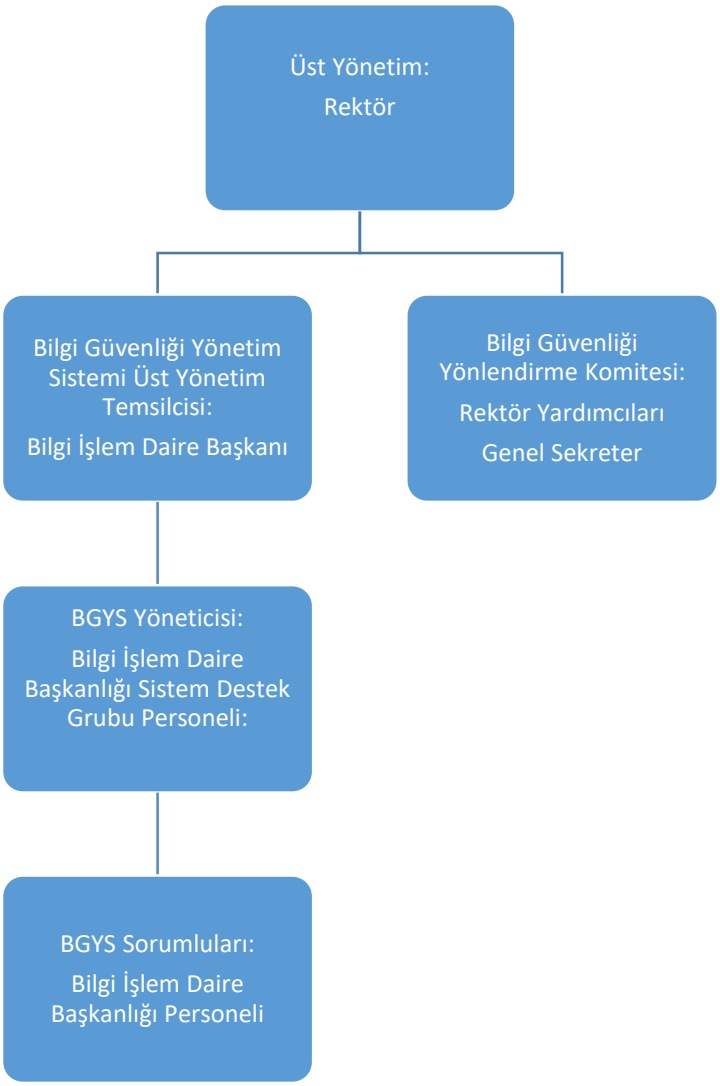
Sivas Cumhuriyet Üniversitesi Bilgi İşlem Daire Başkanlığı 58140 Merkez/SİVAS adresinde bulunan fiziksel yerleşkelerindeki çalışanlarını, iş süreçlerini ve iş süreçlerinde kullandığı ve yönettiği bilgi varlıklarını kapsamaktadır.

6. Sivas Cumhuriyet Üniversitesi Tanıtım

6.1. Kurumumuz

Ülkemizin yüzölçümü bakımından ikinci büyük şehri olan Sivas'ta kurulan Cumhuriyet Üniversitesi, Cumhuriyet'in kuruluşunun 50. yılı anısına, 1974 yılında kanunlaşarak 11000 dönüm arazi üzerinde kurulmuştur 1974 yılında Tıp Fakültesi ile eğitime başlayan Cumhuriyet Üniversitesi bünyesinde bugün, 4 Enstitü, 18 Fakülte, 1 Devlet Konservatuarı, 4 Yüksekokul, 14 Meslek Yüksekokulu ile 50821 öğrenciye hizmet vermektedir.

6.1.1. Kuruluş Yapısı



6.2. Kuruluşun Bağlamı

Kapsam belirleme çalışmalarının yürütülmesinde Bilgi Güvenliği Yönetim Sistemi organizasyonunda görevlendirilmiş personel ile Birimlerin görev tanımlarının incelenmesi ve bu görevleri yürütülmesini etkileyen iç ve dış hususlar, ilgili taraflar, ilgili tarafların beklentileri, kullanılan ara yüzler, bağımlılıklar, diğer kuruluşlar tarafından yürütülen süreçler mülakat yöntemi ile analiz edilmiştir.

6.2.1. Kuruluşun ve Bağlamın Anlaşılması

Misyonu, İnsanı temel alan bir eğitim anlayışı dairesinde, beynelmilel faydalı bilgiye ulaşmayı ve üretmeyi ilke edinen, çevresel, toplumsal ve tarihsel milli ve manevi değerlere sahip ve saygılı, bölgenin ve ülkenin ekonomik, sosyal ve kültürel gelişimine katkı sunan, ulusal ve uluslararası rekabet koşullarında işbirliği ve araştırmalara açık, araştıran, çözümleyen evrensel öğrenci ve akademisyenler yetiştirmektir. Bu misyona uygun olarak Sivas ölçeğinde

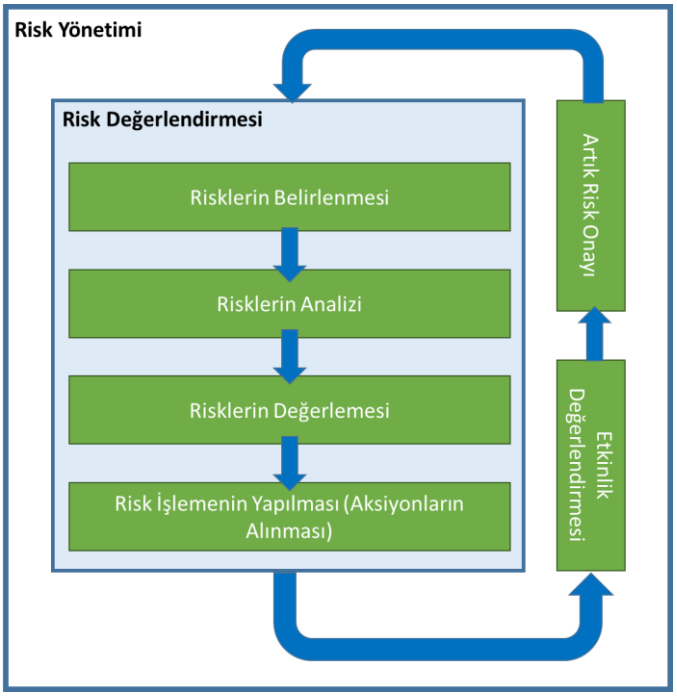
temel görevler üstlenerek bilim ve eğitim merkezi olmak, bu sayede bölgenin ve ülkemizin geleceği ve kalkınmasına katkı sağlamaktır.

7. Planlama

7.1. Risk ve fırsatları belirleme faaliyetleri

7.1.1. Genel

Risk yönetiminde amaç, BGYS kapsamında bilgi güvenliğinin hedeflenen çıktılarını sağlamasıdır. Risk yönetimi süreci yılda en az bir kez gerçekleştirilir. Bunun yanı sıra teknolojide, mimaride, iş süreçlerinde vb. önemli değişikliklere uğrayan varlıklarda ve o varlıkların doğrudan etkilediği veya ilişikli tüm varlıklar üzerinde gerçekleştirilir. Fırsatlar belirlenen riskler göz önünde bulundurularak yönetimin gözden geçirme toplantılarında sunulur. Kullanılan risk yönetim metodu aşağıdaki şekilde belirtilmiştir;



Riskler BGYS sorumluları tarafından gerekli durumlarda teknik uzman yardımı ile belirlenir. Risk belirlemede süreçler incelenir. Süreçlerin incelenmesinde iş akışları ve ilgili varlıkları aşağıdaki kriterlere göre değerlendirilir

- İç / dış hususlar
- İlgili tarafların beklentileri, bağımlılıkları, kullanılan ara yüzler ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetler
- ISO 27001 standardın Ek-A kontrolleri,

- Bilinen iyi uygulamalar
- Teknik testler
- Bilgi güvenliği ihlal olayları,
- Denetim sonuçları
- Tehdit istihbaratları kullanılarak da riskler belirleme işlemi gerçekleştirilir.

8. Destek

8.1. Kaynaklar

8.1.1. Genel

Sivas Cumhuriyet Üniversitesi, kalite yönetim sisteminin oluşturulması, uygulanması, sürekliliğinin sağlanması ve sürekli iyileştirilmesi için ihtiyaç duyulan kaynakları tayin etmiş ve sağlamıştır.

Sivas Cumhuriyet Üniversitesi, ihtiyaç duyulan kaynakları belirlerken, aşağıdakileri değerlendirmiştir:

a) Var olan iç kaynakların yetenekleri ve kısıtlamalarını,

b) Dış tedarikçilerden neyin tedarik edileceğini.

8.1.2. Kişiler

Kurumda personel işe alım, çalışma ve işten çıkış işlemleri, İnsan Kaynakları Müdürlüğü aracılığı ile yürütülür. Bu işlemler sırasında uygulanması zorunlu mevzuat İnsan Kaynakları Müdürlüğü tarafından takip edilir. Personel alımı, görev değişikliği ve istihdamın 657 sayılı Devlet Memurları Kanunu ve 2547 sayılı Yükseköğretim Kanunu'na göre yapılır.

1. İşe alımlarda adayların iş gereksinimleri, erişecekleri bilginin sınıfı, yasa, düzenleme ve etiğe göre geçmiş taramaları yapılır,
2. İşe alımlarda belirtilen özelliklerin doğruluğu (Özgeçmiş, Diploma, sınav vb) kontrol edilir,
3. Kurum personeline bilgi güvenliği sorumluluklarını belirten "Kurumsal Kullanıcı Taahhütnamesi" imzalatılır,
4. Bilgi güvenliği kapsamında rolüne uygun eğitimler verilir ve etkinliği değerlendirilir.

8.1.3. Altyapı

Sivas Cumhuriyet Üniversitesi, proseslerin işletilmesi, ürün ve hizmetlerin uygunluğunu elde etmek için gerekli altyapıyı, tayin etmiş, tedarik etmiş ve sürekliliğini sağlamaktadır.

Altyapı aşağıdakileri içermektedir:

a) Binalar ve ilgili müştemilatı,

b) Donanım ve yazılım dahil makina teçhizatı,

c) Taşıma kaynakları,

d) Bilgi ve iletişim teknolojisi.

8.1.4. Proseslerin işletimi için çevre

Sivas Cumhuriyet Üniversitesi, proseslerin işletilmesi ile ürün ve hizmetlerin uygunluğu için gerekli çevreyi tayin etmiş, tedarik etmişi ve sürekliliğini sağlamaktadır.

Ürün ve hizmetlerin uygunluğunu elde etmek için gerekli uygun bir çevre, aşağıdakiler gibi beşeri ve fiziki unsurların birleşimi olabilir:

a) Sosyal (örneğin, ayrımcılık yapmayan, sakin, cepheleşmemiş),

b) Psikolojik (örneğin, stresi azaltan, tükenmişliği önleyen, duygusal olarak koruyucu),

c) Fiziksel (örneğin, sıcaklık, ısı, nem, ışık, ortamın havası, hijyen, gürültü).

8.2. Yeterlilik

BGYS organizasyonunda görevlendirilen rollere ait eğitim yeterlilikleri aşağıdaki gibidir.

Yeterlilik Şartı / **Rol**	En az 5 yıl bilgi güvenliği sektöründe görev yapma	2 yıllık bilgisayar veya elektronik yüksekokullarından mezun
BGYS Yöneticisi	X	X
BGYS Ekibi		X

Aşağıda belirtilen eğitimler toplu olarak ya da bireysel olarak verilebilir ayrıca eğitim konuları (Eğitim adı) birleştirilebilir. Üçüncü taraf personelin yeterliliğinin belirlenmesi, taraflara bildirilen şartnamelerde belirtilir.

8.3. Farkındalık

Personelin bilgi güvenliği bilincinin artırılması için yapılacak faaliyetler aşağıda tanımlanmıştır.

1. Bilgi güvenliği farkındalık eğitimini tüm personele yılda en az bir kez verilir.
2. İş süreçlerinde görev alan Üçüncü Tarafların eğitim ihtiyaçları BGYS Yöneticisi tarafından belirlenir
3. BGYS Yöneticisi tarafından, yeni başlayan personele Bilgi Güvenliği Farkındalık Eğitimi verilir.
4. Son kullanıcı farkındalık eğitimi en az aşağıdaki başlıkları içerir;
    a) Bilgi Güvenliği Politikaları
    b) Fiziksel Güvenlik

c) Parola Güvenliği
d) Bilgi Sınıflandırma
e) Sosyal Mühendislik
f) İnternet ve İntranet Kullanımı
g) Elektronik Posta Kullanımı
h) Yasal Sorumluluklar
i) Bilgi Güvenliği İhlal Olayları

5. Kullanıcıların farkındalıklarını değerlendirmek amacı ile son kullanıcı farkındalık eğitimi tamamlandıktan en fazla üç ay sonra değerlendirme anketleri yapılır,
6. Eğitim değerlendirme sonuçlarından çalışanların aldığı eğitimi değerlendirmek amacı ile Amaç, Kapsam, Sorumluluk ve Yetki, Yöntem ve Tespit edilen sayısal sonuçlar başlıklarının bulunduğu rapor BGYS Yöneticisi tarafından hazırlanır ve BGYS Üst Yönetim Temsilcisine sunulur,
7. Kurum yerleşkelerinde bilgi güvenliğini sağlamayı, ihlal olaylarını bildirmeyi vb. teşvik edici afişler, posterler vb. materyaller ile bildirimler desteklenir,
8. Özel ilgi grupları ile iletişim halinde olup düzenlenen seminer ve eğitimler takip edilir.

Eğitim Adı / **Rol**	Bilgi Güvenliği Farkındalık Eğitimi	TS EN ISO/IEC 27001 BGYS İç Tetkik Eğitimi	TS EN ISO/IEC 27001 BGYS Temel Eğitimi
Tüm Personel	**X**		
BGYS Yöneticisi		**X**	**X**
BGYS Ekibi			**X**
İç Tetkikçiler		**X**	**X**

8.4. Dokümante Edilmiş Bilgi

8.4.1. Genel

1. Dokümanlar metin ve tablo formatlarında hazırlanır,
2. Hazırlanan metin dokümanlar için aşağıdakileri içerecek şekilde kapak sayfası oluşturulur. Kapak sayfası çerçeve içerisine alınır.
    a. Kuruluş logosu
    b. Kuruluş bilgisi
    c. Doküman Kodu
    d. Doküman Adı
    e. Dokümanın Sınıfı
3. Hazırlanan dokümanlar en az aşağıdaki bölümleri içermelidir
    a. Kapak Sayfası
    b. İçindekiler Tablosu
    c. Amaç
    d. Kapsam
    e. Revizyon Kayıtları
    f. Tanımlamalar ve Kısaltmalar
    g. Uygulama
    h. İlgili Dokümanlar
4. Dokümanlarda, metin formatı için 12 punto, birinci seviye başlık için 18 punto ve kalın, ikinci seviye başlık için 16 punto ve kalın, üçüncü seviye ve daha düşük seviyedeki başlıklar için 14 punto ve kalın Times New Roman yazı tipi kullanılır.
5. Yukarıda belirtilen dokümanlar Metin formatında hazırlanan dokümanlar içindir. Tablo formatında hazırlanan dokümanlar için Üst ve alt başlık veri sayfasında diğer bilgiler “Doküman Açıklaması” sayfasında belirlenir. Tablo formatında hazırlanan dokümanlarda kapak sayfası, içindekiler tablosu, ilgili dokümanlar, kısaltmalar ve tanımlar bölümleri bulunmaz.
6. Dokümanların üst bilgisi aşağıda verilen formata uygun şekilde düzenlenir. Üst bilgide Kurum logosu, doküman adı, doküman numarası, ilk yayın tarihi, revizyon numarası, revizyon tarihi ve toplam sayfadaki sayfa numarası bilgileri yer alır.

	DOKÜMAN ADI			
	Doküman No	**İlk Yayın Tarihi**	**Rev. No / Rev. Tarihi**	**Sayfa No**
	BGYS-XX-YY	gg.aa.yyyy	x / gg.aa.yyyy	x / y

7. Dokümanın alt bilgisi aşağıda verilen formata uygun şekilde düzenlenir. Orta alt alanda ve 16 punto Times New Roman olarak dokümanın sınıfı, altında yer alır.

DOKÜMAN SINIFI

8. Yayın ve revizyon tarihleri dokümanın onaylanıp yayımlandığı tarihler olarak belirlenir. Bu tarihler BGYS Yöneticisi tarafından dokümana eklenir. İlk kez oluşturulan dokümanların revizyon tarihleri boş bırakılır ve revizyon numarası "0" verilir. Doküman her revizyona uğradığında rakam 1 birim artırılarak numaralandırılır.

8.4.2. Dokümanların Gözden Geçirilmesi ve Güncellenmesi

1. BGYS kapsamında oluşturulan tüm dokümanlar yılda en az bir kez ve aşağıdaki durumlar meydana geldiğinde gözden geçirilir ve gerekirse güncellenir.
    a. Teknolojideki değişiklikler
    b. Organizasyonel değişiklikler
    c. Kapsam değişiklikleri
    d. Yasal değişiklikler
    e. Yöntem değişiklikleri
2. BGYS Dokümanları için, değişiklik talebi herhangi bir çalışan tarafından BGYS Yöneticisine kurumsal mail yolu ile bildirilir.
3. Değişiklik yapılan doküman tekrar kontrol, onay ve yayınlanma sürecine girer
4. BGYS Dokümanı üzerinde yapılan değişiklikler, ayrıntılı bir şekilde dokümanın üzerinde bulunan revizyon kayıtları bölümüne girilir;
    - Revizyon No
    - Tarih
    - Revizyon Nedeni
    - Revizyon sayfa No
    - Revize edilen veri
5. Revize doküman yayımlandığı andan itibaren bir önceki doküman geçersiz sayılır.

8.4.3. İç Denetim

8.4.4. Genel

Sivas Cumhuriyet Üniversitesi, bilgi güvenliği yönetim sisteminin aşağıdakilerle ilgili durumunu belirlemek için planlanan aralıklarda iç denetimler yapmaktadır:

1. Sivas Cumhuriyet Üniversitesi'nin bilgi güvenliği yönetim sisteminin şartlarına,
2. ISO 27001:2013 standartlarının şartlarına.

8.4.5. İç Denetim Programı

1. TS ISO/IEC 27001 BGYS faaliyetleri, yılda asgari bir defa olmak üzere tetkik edilir, ancak gerektiğinde yıl içerisinde birden fazla tetkik gerçekleştirilebilir.
2. İç tetkik, kapsam dâhilinde gerçekleştirilir.
3. Planlanan tetkik için, süreçle ilgili tüm fonksiyonel uzmanlık alanlarında değerlendirme yapabilecek tetkikçi ya da tetkikçiler seçilir.
4. Tetkik süreleri ve tetkik ekibindeki tetkikçi sayısı, tetkik kapsamı ve geçmiş tetkiklerdeki durumu da dikkate alınarak BGYS Yöneticisi tarafından belirlenir.
5. Tetkikler, en az TS ISO/IEC 27001 BGYS Temel Eğitimi ve İç Tetkikçi Eğitimi almış ve değerlendirme sonucunda başarılı olmuş kişilerden ya da Baş Tetkikçi Sertifikalı tetkikçiler tarafından gerçekleştirilir.
6. Tetkiklerin tarafsızlığı için tetkik ekibi, tetkik edilecek bölüm ve faaliyetlerden bağımsız olarak seçilir.
7. Tetkikler için kurum içi ya da kurum dışı kaynaklar kullanılabilir.
8. Tetkikler iki aşamadan oluşur. Birinci aşama standarda uyum için gereksinimlerin belirlenmesi ikinci aşama belirlenen gereksinimlerin uygulanması üzerine gerçekleştirilir.
9. Tetkikçiler tarafsız ve objektif davranır.
10. Tetkikler sırasında tetkikçiler ihtiyaç halinde uzman çalışanlardan destek alır.
11. Tetkik sonucunda tespit edilen bulgular, Düzeltici ve İyileştirici Faaliyet Prosedürüne uygun şekilde Düzeltici Faaliyet Formu doldurarak takip edilir.
12. İç tetkik sonrası elde edilen sonuçlar raporlanır.

8.4.6. İyileştirme

8.4.7. Genel

Düzeltici ve İyileştirici Faaliyetler ile ilgili tüm işlemler DİF formu kullanılarak gerçekleştirilir ve kayıtları Doküman Yönetim Prosedürü ne uygun olarak saklanır. Onay ve bildirim işlemleri kurumsal e-posta kullanılır.

8.4.8. Uygunsuzluğun ya da İyileştirilecek Konuların Tespit Edilmesi

Uygunsuzluk konuları aşağıda yer alan başlıklar sonucunda ortaya çıkabilir:

1. İç tetkik sonuçları
2. Dış tetkik sonuçları
3. İhlal olayı bildirimleri
4. Arıza raporları
5. Sözleşmeler
6. Çalışanların önerisi
7. İstatistikî bilgiler
8. Halkın ve ilgili tarafların ihtiyaç beklentileri ve şikâyetleri
9. Yasal ve diğer şartlarının karşılanmadığı durumlar
10. Acil durumlar
11. Eğitim Etkinlik Değerlendirmesi
12. Hedef İzlemeleri
13. Bir önceki yönetim gözden geçirme sonuçlarının değerlendirilmesi
14. Veri analizi ve raporları
15. Teknolojik gelişmeler
16. Teknik zafiyet testleri
17. Anket sonuçları.

8.4.9. Düzeltici ve İyileştirici Faaliyet Ön Değerlendirmesinin Yapılması

1. 5.1 maddesinde belirtilen yollardan gelen bildirimler BGYS Yöneticisi tarafından değerlendirilir ve gerekli görülürse DİF başlatılır veya düzeltme faaliyeti gerçekleştirildikten sonra DİF başlatılır. Örneğin; istemcilerde anti virüs programı bozulmuş ise yeniden yüklenerek sorun çözülür daha sonrasında bu bozulma için DİF başlatılır, kök neden analizi yapılarak sorunun bir daha yaşanmaması için önlemler alınır.
2. DİF talebi başlatılmadan önce BGYS Yöneticisi uygunsuzluğun durumuna göre ilgili birim yöneticilerini ve / veya BGYS Üst Yönetim Temsilcisini toplantıya çağırabilir.
3. BGYS Yöneticisi DİF ile ilgili benzer uygunsuzlukların başka birimlerde de var olup olmadığını veya olasılıkla gerçekleşip gerçekleşmeyeceği hakkında araştırma yapar ve gerekirse DİF talebinin kapsamı genişletilir.
4. DİF formu oluşturulduktan sonra ilgili birim yöneticisine gerekli çalışmaları yürütmesi için iletilir.