KAPADOKYA ÜNİVERSİTESİ

Akıl - Ahlak - Adalet - Adap

BİLGİ GÜVENLİĞİ EL KİTABI

Doküman No: BGEK-001
Yayın Tarihi: Aralık 2017
Revizyon No: 00
Revizyon Tarihi:

İÇİNDEKİLER

ÖNSÖZ 1

REVİZYON LİSTESİ 2

DAĞITIM LİSTESİ 3

ONAY 4

A. GENEL 5

B. BİLGİ GÜVENLİĞİ EL KİTABI REVİZYON VE DAĞITIMI 5

C. ÜNİVERSİTEMİZİN TANITIMI: 5

BİLGİ GÜVENLİĞİ POLİTİKAMIZ 7

1. AMAÇ 13

2. KAPSAM 13

3. HARİÇ TUTULAN STANDART MADDELERİ 13

4. ÜNİVERSİTEMİZİN BAĞLAMI 14

4.1. Kuruluş ve Bağlamının Anlaşılması: 14

4.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması 15

4.3. Bilgi Güvenliği Yönetim Sistemi Kapsamının Belirlenmesi 16

4.4. Bilgi Güvenliğ Yönetim Sistemi ve Prosesleri 16

5. LİDERLİK 17

5.1. Liderlik ve Taahhüt 17

5.2. Politika 17

5.3. Kurumsal Görev, Sorumluluklar ve Yetkiler 18

6. PLANLAMA 19

6.1. Risk ve Fırsatları Belirleme 19

6.2. Bilgi Güvenliğ Amaçları ve Bu Amaçları Başarmak için Planlama 20

7. DESTEK 21

7.1. Kaynaklar 23

7.2. Yeterlilik 23

7.3. Farkındalık 23

7.4. İletişim 25

7.5. Yazılı Bilgiler 25

8. İŞLETİM 29

8.1. İşletimsel Planlaması ve Kontrolü 29

8.2. Bilgi Güvenliği Risk Değerlendirme 30

8.3. Bilgi Güvenliği Risk İşleme ..... Hata! Yer işareti tanımlanmamış.

9. PERFORMANS DEĞERLENDİRME 31

9.1. İzleme, Ölçme, Analiz ve Değerlendirme 31

9.2. İç Tetkik 32

9.3. Yönetimin Gözden Geçirmesi 33

10.İYİLEŞTİRME 34

10.1. Uygunsuzluk ve Düzeltici Faaliyet 34

10.2. Sürekli İyileştirme 34

ÖNSÖZ

Bu El Kitabı Kapadokya Üniversitesinin bilgi güvenliği sağlanması için programlarını, politikalarını ve amaçlarını ortaya koyar. Üniversitemizde yürütülen eğitim hizmetleri için Bilgi Güvenliği bir yaşam tarzı olarak benimsenmiştir. Üniversitemizden hizmet alan kişi, kurum ve kuruluşlara, dürüst ve prensipli kararlarla Bilgi Güvenliği hizmet vermeyi kendisine amaç edinmiştir.

Bilgi Güvenliği Yönetim sistemi ilkeleri doğrultusunda çalışmalarını sürdürmeye başlamış olan Üniversitemiz TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemini etkin bir şekilde uygulamaya başlamıştır.

Kapadokya Üniversitesi misyonu ve vizyonu çerçevesinde vermiş olduğu eğitim hizmetlerinin Bilgi Güvenliği seviyesini her zaman en üst seviyede tutmayı ilke edinmiştir.

REVİZYON LİSTESİ

Doküman No	Rev. No	Revizyon Tarihi	Revizyon Sebebi	Revize Eden

DAĞITIM LİSTESİ

DOKÜMAN NO	BİRİM	DAĞITIM ŞEKLİ	KONTROLLÜ KONTROLSÜZ
BGEK-001	Tüm Üniversite Personeli	Elektronik	Kontrolsüz

ONAY

Bu El Kitabının, TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi gereklerine göre çalışmalarını yürüten Kapadokya Üniversitesinin; Bilgi Güvenliği Politikasını, Amaçlarını (Hedeflerini) ve Sistem Dokümantasyonunu kapsadığını taahhüt ederiz.

Üniversite yönetimi, TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardı gereği aşağıdaki konuları taahhüt eder. Bunlar;

a) Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kuruluşun stratejik amaç ve hedefleri ile uyumlu olmasının temin edilmesi,

b) Bilgi güvenliği yönetim sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesinin temin edilmesi,

c) Bilgi güvenliği yönetim sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesi,

ç) Etkin bilgi güvenliği yönetim sisteminin şartlarına uyum sağlamanın öneminin duyurulması,

d) Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılmasının temin edilmesi,

e) Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi, eğitilmesi ve desteklenmesi,

f) Sürekli iyileştirmenin desteklenmesi

g) Kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rollerinin desteklenmesi.

Referans: BGYS-PR-020 BGYS Uyum Prosedürü

A. GENEL

Bilgi Güvenliği El Kitabı'nın revizyonu ve dağıtımı Kalite ve Stratejik Planlama Dairesinin sorumluluğundadır.

Birimlerin Revizyon istekleri Dokümantasyon Prosedürü esaslarına göre değerlendirilir. Ayrıca Bilgi Güvenliği Yönetim Temsilcisi, Bilgi Güvenliği El Kitabını yılda en az bir defa Yönetimi Gözden Geçirme Toplantısı öncesi gözden geçirir gerekli görülen değişiklikleri yapar ve güncellenmesi gereken dokümanların güncelleştirilmesini sağlayarak üst yönetimin onaya sunar.

B. KALİTE EL KİTABI REVİZYON VE DAĞITIMI

Bilgi Güvenliği El Kitabında yapılan revizyonun duyurulması işleminde aşağıdaki işlemler takip edilir.

1. Yapılan tüm revizyonlar, tüm birim personeline web sitesi aracılığı ile duyurulur.
2. Revizyonlar, “Revizyon Listesine" işlenir ve bir sıra numarası verilir.
3. Gerçekleştirilen revizyonlar revizyon takip formu ile kayıt altına alınır. Kalite ve Stratejik Planlama Dairesi tarafından arşivlenir.
4. İç denetimler sırasında tüm birim personellerinin en son revizyonu, Bilgi Güvenliği El Kitabına ulaşabildikleri kontrol edilir.
5. Revizyon yapılan sayfalara revizyon numaraları (01, 02, 03 ....) ve revizyon tarihleri işlenir.

C. ÜNİVERSİTEMİZİN TANITIMI:

1. Üniversitenin Adı

KAPADOKYA ÜNİVERSİTESİ

2. Logosu

KAPADOKYA ÜNİVERSİTESİ
Akıl - Ahlak - Adalet - Adap

3. Kullanılan Adı

KAPADOKYA ÜNİVERSİTESİ

4. Kuruluş Adresi

50420 - Mustafapaşa, Ürgüp / Nevşehir

Telefon: 0 (384) 353 50 09 Faks: 0 384 353 51 25

Sabiha Gökçen Havalimanı C – Blok, 34912 Pendik / İstanbul

Telefon: 0 (216) 588 00 10 Faks: 0 (216) 588 00 12

www.kapadokya.edu.tr

5. Kuruluş Tarihi

1 Temmuz 2017 tarihli ve 30111 sayılı Resmî Gazete ’de yayımlanmış olan 7033 sayılı Sanayinin Geliştirilmesi ve Üretimin Desteklenmesi Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanunun 21. Maddesi ile 28/3/1983 tarihli 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanununa eklenen Ek Madde 173 ile Kapadokya Üniversitesi kurulmuştur.

6. Faaliyet Konusu

Kapadokya Üniversitesinde yaygın-örgün eğitim, araştırma ve idari hizmetler verilmektedir.

7. Tarihçe

Kapadokya Üniversitesinin geçmişi, Bakanlar Kurulu’nun 03.07.2008 tarih ve 2008/13861 sayılı kararı ile kurulmuş bulunan Kapadokya Meslek Yüksekokuluna dayanmaktadır.

Kapadokya Meslek Yüksekokulu, 7033 sayılı Sanayinin Geliştirilmesi ve Üretimin Desteklenmesi Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanunun 49. geçici maddesi ile tüzel kişiliği sona erdirilerek Kapadokya Üniversitesine bağlanmış, Meslek

Yüksekokulunun tüm öğrenci, öğretim elemanı ve mal varlığı yeni kurulan Üniversiteye devrolmuştur.

Kapadokya Üniversitesi, yönetim ve organizasyonu, 2547 sayılı Yükseköğretim Kanunu, Vakıf Yükseköğretim Kurumları Yönetmeliği ve sair mevzuat uyarınca faaliyet göstermektedir.

Mütevelli Heyet, Üniversitenin en yüksek karar organı olup Üniversitenin tüzel kişiliğini temsil etmektedir. Mütevelli Heyeti üyeleri, Vakıf yönetim organı tarafından, yaş sınırlaması hariç devlet memuru olma niteliklerine sahip adaylar arasından dört yıl süre için seçilen üyelerden oluşmaktadır. Mütevelli heyet toplantılarının koordinasyon, sekretarya ve raportörlüğü Mütevelli Heyet Koordinatörü tarafından yürütülür.

Rektör, Üniversitenin en üst akademik yöneticisidir. Rektör, mütevelli heyetinin Yükseköğretim Kuruluna teklifi ve YÖK'ün olumlu görüşü üzerine Cumhurbaşkanı tarafından atanır. Rektör, eğitim faaliyetlerinin en üst düzeyde yürütülmesi, ileriye dönük gelişmelerin sağlanması ile eğitim ve öğretimin Bilgi Güvenliğinin arttırılmasından sorumludur. Üniversite organları; Rektör, Senato ve Üniversite Yönetim Kurulundan oluşmaktadır. Stratejik Plan Hazırlama Kurulu, Rektöre bağlı organlar olarak stratejik planlama ve Bilgi Güvenliği yönetiminden sorumludur.

İdari yapı genel sekreter, genel sekretere bağlı koordinatörlükler, daire başkanları, birim sorumluları ve diğer görevlilerden oluşmaktadır.

BİLGİ GÜVENLİĞİ POLİTİKALARIMIZ

Üniversitemizin politikaları, Bilgi Güvenliği Politikaları Prosedürüne uygun olarak hazırlanır. Üniversitemizde TS EN ISO 27001 Bilgi Güvenliği kapsamında aşağıdaki BGYS-PR-008 Bilgi Güvenliği Politikaları Prosedürüne uygun olarak oluşturmuştur. Bunlar;

- Bilgi Güvenliği Politikası,
- Erişim Kontrol Politikası,
- Temiz Masa Temiz Ekran Politikası,
- Güvenli Geliştirme Politikası,
- Tedarikçi İlişkileri Politikası,

Bilgi Güvenliği Politikası,

Üniversitemiz sahip olduğu tüm fiziksel ve elektronik bilgi varlıklarının gizliliğinin ve bütünlüğünün korumasını taahhüt etmektedir.

Üniversitemiz bilgi güvenliği gereksinimlerini sağlamak için değişime açık, iyi eğitim almış, konusunda yetkin personel istihdamını sağlayacaktır. Ayrıca bilgi güvenliğinin sağlanması amacıyla gerekli olan alt yapısını oluşturmak ve sürekliliğini sağlamak için finansmanı, yeterli donanımı ve altyapıyı bulunduracaktır.

Bilgi güvenliği sistemi faaliyetlerimiz, acil durum planları, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimi gibi konulardan oluşmaktadır.

Risk değerlendirmeleri sonucunda amaçlarımızı belirleyip bu amaçların başarılması için gerekli olan kaynaklar ve şartlar sağlanacaktır. Yapılan risk değerlendirmeleri sonucunda sistemde tespit edilen açıklar ve tehditler bertaraf edilerek öğretim elemanlarımızın, idari personellerimizin, öğrencilerimizin ve üniversiteye gelecek misafirlerimizin bilgilerinin bilgi güvenliği politikamız gereği korunması sağlanacaktır.

Akademik ve idari personelimizin, Bilgi Güvenliği politikamızı yerine getirmek için Bilgi Güvenliği Yönetim Sistemi şartlarını çalışma biçimi haline getirmeleri sağlanacaktır. Tüm personel ve üçüncü tarafların Bilgi Güvenliği Yönetim Sistemi ile ilgili uygun eğitimleri alması sağlanacaktır.

Bilgi güvenliği ile ilgili uygulanabilir şartlar ve bu şartların getirdiği fırsatlar ve gereklilikler yerine getirilecek ve bu şartlar sürekli iyileştirilecektir. Akademik ve idari personelimizin (tedarikçilerimizin personelleri dahil) ve tüm ilgili tarafların bu sisteme adaptasyonu sağlanacaktır.

Erişim Kontrol Politikası,

Üniversitemizin iç taleplerine zamanında ve doğru çözümler bulabilmemiz için yasal mevzuata uygun şekilde verinin bütünlüğünün sağlanması için:

- Oryantasyon aşamasında personele gerekli bilgiler aktarılmış,
- Gerekli altyapı ve donanım belirlenmiş,
- Gerekli altyapı ve donanımın kesintisiz olarak sağlanması için, gerekli kaynaklar ayrılmış,
- Üniversitemizin, akademik ve idari personeller, öğrenciler ve üniversitemize gelen misafirlerimizin bilgilerinin korunması açısından yapılması gerekenler personelimize eğitimlerle aktarılmış, üniversite çalışanlarımıza "iş sözleşmeleri" ile sorumlulukları yazılı hale getirilmiş,
- Tüm verilerin yedeklenmesi amacıyla gerekli alt yapı belirlenip, sorumlular tanımlanmış,
- Network üzerinde gerekli erişim işlemleri sınırlandırılmış,
- Bilgi güvenliği konusundaki 3 temel prensibi gizlilik, bütünlük ve yetkililerce erişilebilirlik prensipleri belirlenmiştir.

Temiz Masa Temiz Ekran Politikası,

Temiz Masa Temiz Ekran Politikamızın amacı, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamaktır.

Akademik ve idari personelin aşağıdaki şartlara uygun davranmaları gerekmektedir.

1. Çalışma saatleri dışında bilgisayarlar kapalı ya da kilitli şekilde bırakılmalıdır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır.(Ekran koruyucu 5-10 dk arasında devreye girmelidir ve şifre koruması olmalıdır.)
2. Yazıcıların üzerinde kişisel bilgileri ve gizli bilgileri içeren dokümanlar(müsvedde olsalar bile)bırakılmamalıdır.
3. Yazıcı ile işlem tamamlandığından yazıcı kilit ekranına alınmalıdır.
4. Yazıcı şifreleri personel dışındakilerle paylaşılmamalıdır.
5. Mesai bitiminde çalışma masası üzerinde kurum veya kişisel bilgileri içeren bir evrak bırakılmamalıdır.
6. Kuruma ait dokümante edilmiş gizli bilgiler kilitli ortamda tutulmalıdır.
7. Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.
8. Kuruma ait antetli kağıtlar kilitli dolaplarda tutulmalıdır.
9. Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenir.
10. Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.
11. Bilgisayarlara ait olan şifreler kesinlikle kâğıt ortamlara yazılı bir şekilde bırakılmamalı.

Güvenli Geliştirme Politikası,

Güvenli geliştirme, güvenli hizmet için bir gerekliliktir. Bunun için öncelikle güvenli geliştirme ortamları kullanılacaktır. Eğitim-öğretim hizmetlerimizin yaşam döngüsü dâhilinde, tasarım aşamasında güvenlik gereksinimleri belirlenerek, bu güvenlik gereksinimlerinin uygulanması sağlanacaktır. Eğitim-öğretim hizmetlerimizde güvenlik kontrol noktaları oluşturularak yapılan testlerde bu güvenlik kontrollerine uyulması sağlanacaktır. Tüm geliştiriciler açıklıklardan kaçınma, açıklıkları bulma ve düzeltme konusunda kendilerini geliştireceklerdir.

Tedarikçi İlişkileri Politikası,

Tedarikçilerimizin, Kapadokya Üniversitesinde uygulanan Bilgi Güvenliği Yönetim Sistemi Şartlarına uygun olarak faaliyet göstermesini beklemekteyiz. Özellikle bilgi sistemlerimize erişim sağlayan bakım hizmetleri gerçekleştiren ya da sistemi temini sağlayan tedarikçilerin bu konulara uyumu büyük önem göstermektedir. Uyumun sağlanmaması yasal yaptırımları beraberinde getirecektir.

Tedarikçilerimizin özellikle yapılacak tedarikçi sözleşmelerine uyum sağlaması önemlidir. Bu sözleşmeler verilerini korumakla yükümlü olduğumuz akademik personel, idari personel, öğrencilerimiz ve hizmet alıcıları için ayrı önem taşımaktadır.

Bu kapsamda;

- Tedarikçilerimizin yasal gereklilikleri yerine getiren ve bu politika ve kurallar ile beraber iş etiği ile bağlantılı olan diğer tüm dokümanlardaki gerekliliklere bağlı tedarikçiler olması gerekmektedir.
- Tedarikçi seçiminde; mali performans, tecrübe, teknik yeterlilik vb. kriterlerin yanında bu alanda olumlu bir geçmişe sahip olmaları ve önceki yıllara ait değerlendirme sonuçları dikkate alınır.
- Tedarikçi seçimi ve yönetimi için ilgili daire başkanları onaylı tedarikçi listesi hazırlama, yönetme ve takip sistemlerinin kurulmasından sorumludur.
- Birlikte çalışmaya karar verdiğimiz tedarikçilerimizi seçerken objektif kriterlere göre değerlendiriyoruz. Kapadokya Üniversitesi olarak tedarikçilerimiz ile iş ilişkilerimizde karşılıklı değer yaratmayı hedeflemekteyiz.
- Kapadokya Üniversitesi olarak tedarikçilerimizin yasalara, kurallara, düzenlemelere bağlı kalmasını hedefleriz. Tedarikçilerin, birlikte çalıştıkları tedarikçilerin ve taşeronlarının işle ilgili uygulamalar konusunda bilgi sahibi olmasını bekleriz.

Kapadokya Üniversitesi, bu kurallara uymayan tedarikçilerle ilişkilerini sonlandırma hakkını saklı tutar.

Referans: BGYS-PR-008 Bilgi Güvenliği Politikaları Prosedürü
BGYS-PR-012 Erişim Kontrolü Prosedürü
BGYS-PR-017 Tedarikçi İlişkileri Prosedürü
Bİ.PL.001 Bilgi Güvenliği Politikası,
Bİ.PL.002 Erişim Kontrol Politikası,
Bİ.PL.003 Temiz Masa Temiz Ekran Politikası,
Bİ.PL.004 Güvenli Geliştirme Politikası,
Bİ.PL.005 Tedarikçi İlişkileri Politikası,

1. AMAÇ

Üniversitemiz, yürürlükteki mevzuat şartlarına ve TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemine uygun şekilde faaliyetlerini sürdürerek, hizmet alanların beklentilerine en iyi şekilde cevap verebilmeyi amaç edinmiştir. Bu doğrultuda sistemin sürekli iyileştirilmesi ve etkinliğinin artırılması amacıyla Bilgi Güvenliği Yönetim Sistemini kurmuş ve bu El Kitabını sistemin etkin olarak kullanılması ve çalıştırılması için oluşturmuştur.

2. KAPSAM

Üniversitemiz tarafından mevzuat çerçevesinde yerine getirilen faaliyetlerin tümü TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamına alınmıştır. Sistemimiz; 50420-Mustafapaşa, Ürgüp/Nevşehir ve Sabiha Gökçen Havalimanı C–Blok, 34912 Pendik/İstanbul adreslerinde faaliyette bulunan Kapadokya Üniversitesinin tüm birimleri kapsayacak şekilde kurulmuştur.

3. HARİÇ TUTULAN STANDART MADDELERİ

Kapadokya Üniversitesi Rektörü ve Bilgi Güvenliği Yönetim Temsilcisi kapsam dışında tutulacak olan standart maddelerin tespitinden sorumludur. Üniversitemizde, TS EN ISO 27001 Bilgi Güvenliği Yönetim Sisteminde **hariç tutulan madde bulunmamaktadır**.

4. ÜNİVERSİTEMİZİN BAĞLAMI

4.1. Kuruluş ve Bağlamının Anlaşılması:

Kapadokya Üniversitesi olarak stratejik hedeflerimiz ve Bilgi Güvenliği politikamız doğrultusunda Bilgi Güvenliği Yönetim Sistemimizin amaçlanan hedeflere ulaşabilme yeteneğini etkileyen iç ve dış hususlar aşağıdaki gibi tayin edilmiştir.

Üniversitemizde iç husus olarak;

- İdare, üniversitemize ilişkin yapı, roller ve yükümlülükler,
- Yerine getirilecek politikalar, hedefler ve stratejiler,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri,
- Üniversitemizin kültürü,
- Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrı resmi),
- Kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller,
- Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.
- Fiziksel altyapı yeterliliği,

Üniversitemizde dış husus olarak;

- YÖK tarafından belirlenen kurallar,
- Eğitim Hizmetleri ve Araştırma-Geliştirme faaliyetleri için yayınlanan yasal şartlar (Kanun, Yönetmelik, Talimat, Genelge, Tebliğ vb.)
- Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,
- Kuruluşun hedefleri üzerinde etkisi bulunan kilit sürücüler ve eğilimler,
- Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri.

Belirlenen iç ve dış hususlarla ilgili bilgi izlenmekte ve Yönetimi Gözden Geçirme toplantılarında değerlendirilmektedir.

4.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

a) Bilgi Güvenliği Yönetim Sistemi ile İlgili Taraflar

Üniversitemizde, Bilgi Güvenliği Yönetim Sistemi ile ilgili taraflar:

1) Tüzel Kişilik,

2) Öğretim Elemanları, İdari Personel ve Sözleşmeli Personeller,

3) Tedarikçiler,

4) Öğrenciler,

5) Dış Paydaşlar

b) Tarafların Bilgi Güvenliği İle İlgili Gereksinimleri:

Bilgi Güvenliği Yönetim Sistemi ile ilgili beklentileri:

İlgili Taraf	Beklentiler
Tüzel Kişilik	- Prestijinin korunması, - Elde ettiği bilgi birikiminin korunması, - Yasal şartlara uyum,
Çalışanlar	- Uygun çalışma şartları,
Tedarikçiler	- Rahat hizmet verebilme, - Zamanında ödeme alma, - Çalışma sürekliliği,
Öğrenciler	- Şartlara uygun hizmetlerin alınması, - Hizmette sürekliliğin sağlanması, - Eğitim ve Öğrenim için gerekli imkânların sağlanması (yurt, yemekhane, kütüphane, sosyal faaliyetler vb.)
Dış Paydaşlar	- Yasal şartlara uyum - Geri bildirim sistemi - İstek ve şikâyetlerin dikkate alınması

Üniversitemizde ilgili tarafları ve şartlarını yıllık periyodlarda yapılan Yönetim Gözden Geçirme toplantıları ile gözden geçirmektedir.

4.3. Bilgi Güvenliği Yönetim Sistemi Kapsamının Belirlenmesi

Kapadokya Üniversitemizin mevcut faaliyet alanları için, tarafların şartlarını karşılamak amacıyla TS EN ISO 27001 standardına uygun olarak bir Bilgi Güvenliği Yönetim Sistemi kurulmuştur. Kurulan sistem üniversitemizin tüm bölümlerini, çalışanları, dış hizmet aldığımız tedarikçilerimiz, hizmet verdiğimiz öğrenciler ve üniversitemize gelen misafirlerimizi/ziyaretçilerimiz için uygulanmaktadır.

Bilgi Güvenliği Yönetim Sistemimizin kapsamı üniversitemiz, öğrencilerimiz, tedarikçilerimiz ve personelimiz için sözlü ve elektronik ortamdaki tüm bilgi çeşitlerini içermektedir.

Kapadokya Üniversitesi olarak TS EN ISO 27001 Bilgi Güvenliği Yönetim Sisteminin kapsamı belirlenirken aşağıdaki konuları dikkate alınmıştır. Bunlar;

- İç ve dış hususlar(Madde 4.1.),
- İlgili tarafların ihtiyaç ve beklentileri(Madde 4.2.),
- Üniversitemiz tarafından gerçekleştirilen faaliyetler arasındaki ara yüzler, bağımlılıklar ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetler

Üniversitemizin kapsamı ve hariç tutulan maddeler ilgili bölümlerde tanımlanmıştır.

4.4. Bilgi Güvenliği Yönetim Sistemi ve Prosesleri

Üniversitemizde, TS EN ISO 27001 standardın şartlarına uygun olarak, ihtiyaç duyulan prosesler ve bunların birbiri ile etkileşimi **(Proses Etkileşim Planları)** dâhil, bir Bilgi Güvenliği yönetim sistemi kurularak uygulamakta, sürekliliği sağlamakta ve sürekli iyileştirilmektedir.

5. LİDERLİK

5.1. Liderlik ve Bağımlılık

Üst yönetim aşağıdakileri yerine getirerek Bilgi Güvenliği Yönetim Sistemi için liderlik ve bağımlılık göstermiştir:

a) Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kuruluşun stratejik amaç ve hedefleri ile uyumlu olmasının temin edilmesi (Madde 7 Politikalarımız),

b) Bilgi güvenliği yönetim sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesinin temin edilmesi (Madde 4),

c) Bilgi güvenliği yönetim sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesi (Madde 7.1.),

ç) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sisteminin şartlarına uyum sağlamanın öneminin duyurulması (Madde 7.2, Madde 7.3, Madde 7.4.),

d) Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılmasının temin edilmesi (Madde 8),

e) Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesi (Madde 9),

f) Sürekli iyileştirmenin desteklenmesi (Madde 10),

g) Kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rollerinin desteklenmesi (Madde 5.3),

5.2. Politika

5.2.1. Bilgi Güvenliği Politikasının Oluşturulması

Üst yönetim Bilgi Güvenliği Politikasını oluşturmuştur. Buna göre politika:

a) Üniversitemizin amacına uygun,

b) Bilgi güvenliği amaçlarını içeren (Bk. Madde 6.2) veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlayan,

c) Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt içeren,

ç) Bilgi güvenliği yönetim sisteminin sürekli iyileştiren bir yapıya sahiptir.

5.2.2. Bilgi Güvenliği politikasının duyurulması

a) Bilgi Güvenliği Yönetim Sistemi kapsamında politikalar dokümante edilmiştir. Bunlar;

- Bilgi Güvenliği Politikası (Bİ.PL.001),
- Erişim Kontrol Politikası (Bİ.PL.002),
- Temiz Masa Temiz Ekran Politikası (Bİ.PL.003),
- Güvenli Geliştirme Politikası (Bİ.PL.004),
- Tedarikçi İlişkileri Politikası (Bİ.PL.005),

b) Verilen eğitimler ile Üniversitemiz içerisinde duyurulmuştur.

c) Web sitesinde yayınlanarak ilgili tarafların erişimine açılmıştır.

5.3. Kurumsal Görev, Sorumluluklar ve Yetkiler

Üniversitemizde genel yapısı Organizasyon Şeması üzerinden tanımlanmıştır. Organizasyon şemasına uygun olarak da bölümler bazında Görev, Yetki ve Sorumluluklar dokümante etmiştir.

Ayrıca:

a) Bilgi Güvenliği Yönetim Sisteminin, bu standardın şartlarını karşılanması güvence altına alınmıştır.

b) Bilgi Güvenliği yönetim sisteminin performansı ve iyileştirme için fırsatlar ile ilgili raporlama yapılması planlanmıştır.

Bilgi Güvenliği Yönetim Temsilcisi görev, yetki ve sorumlulukları tanımlanmıştır. Bu çalışmalar detaylı olarak Bilgi Güvenliği Organizasyon Prosedürü' nde tanımlanmıştır.

Referans: BGYS-PR-009 Bilgi Güvenliği Organizasyon Prosedürü

6. PLANLAMA

6.1. Risk ve Fırsatları Ele Alan Faaliyetler

6.1.1. Genel:

Üniversitemizde, Bilgi Güvenliği yönetim sistemi planlamasında Madde 4.1'de atıf yapılan hususları, Madde 4.3'de atıf yapılan şartları ve aşağıda belirtilen risk ve fırsatların değerlendirilmesini tayin etmek için Risk Analizi Prosedürü oluşturmuş ve uygulamaktadır:

a) Bilgi Güvenliği yönetim sisteminin amaçlanan çıktısına/çıktılarına ulaşabileceğine güvence vermek,

b) İstenmeyen etkileri önlemek veya azaltmak,

c) Sürekli iyileşmenin başarılması,

Üniversitemiz aşağıdakileri planlamaktadır:

a) Bu risk ve fırsatları belirleme faaliyetlerini,

b) Faaliyetleri Bilgi Güvenliği yönetim sistem prosesleri içerisine nasıl entegre edeceği ve uygulayacağını,

c) Bu faaliyetlerin etkinliğini nasıl değerlendireceğini.

Risk ve fırsatları ele alma faaliyetleri, ürün ve hizmetlerin uygunluğuna potansiyel etkisi ile orantılıdır.

Üniversitemiz risk analizi için risk kriterleri oluşturulmuş, tekrarlanan riskler için geçerli ve karşılaştırılabilir sonuçlar üretmesi için yöntemler belirlenmiştir.

Risklerin analizi sonucunda risk seviyeleri belirlenmiş ve bu risklere ilişkin önlemler Risk Analizi içerisinde belirlenmiştir.

Üniversitemizde bilgi güvenliğinin sürekli hale gelmesi için BGYS-PR-019 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları Prosedürü' nde tanımlanmıştır.

Referans: BGYS-PR-019 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları Prosedürü

KPS.KYS.PR.006 Risk Analizi Prosedürü

6.1.2. Bilgi Güvenliği Risk Değerlendirme

Üniversitemiz, akademik ve idari birimlerinde Bilgi Güvenliğini sağlamak ve geliştirmek için Risk ve Fırsatları Belirleme Prosedürü oluşturulmuş ayrıca risk değerlendirme süreçlerini aşağıdaki maddelere uygun olarak tasarlamıştır.

Bilgi Güvenliği Risk Değerlendirme için:

a) Aşağıdakileri içeren bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi:

1. Risk kabul kriterleri,
2. Bilgi güvenliği risk değerlendirmesi yapılması için kriterler,

b) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi,

c) Bilgi güvenliği risklerinin tespit edilmesi:

1. Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme prosesinin uygulanması,
2. Risk sahiplerinin belirlenmesi,

d) Bilgi güvenliği risklerinin analiz edilmesi:

1. Madde 6.1.2 c) 1) de belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi,
2. Madde 6.1.2 c) 1) de belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi,
3. Risk seviyelerinin belirlenmesi,

e) Bilgi güvenliği risklerinin değerlendirilmesi:

1. Risk analizi sonuçlarının Madde 6.1.2 a)'da oluşturulan risk kriterleri ile karşılaştırılması,
2. Analiz edilen risklerin risk işleme için önceliklendirilmesi,

Üniversitemiz bilgi güvenliği risk değerlendirme süreci ile ilgili olarak yazılı bilgilerin muhafaza edileceği yapıyı kurmuş ve işletmektedir.

6.1.3. Bilgi Güvenliği Risk İşleme

Kapadokya Üniversitesi aşağıdakileri gerçekleştirmek için bir bilgi güvenliği risk işleme süreci tanımlamış ve uygulamaktadır. Bunlar;

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi,

b) Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi,

c) Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan "tüm kontroller" ve "referans kontrol amaçları ve kontroller" karşılaştırılması ve gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması,

d) Gerekli kontrollerin gerekçelendirmesi, uygulanıp uygulanmadıklarını ve "referans kontrol amaçları ve kontroller" kontrollerin dışarıda bırakılmasının gerekçelendirmesini içeren bir Uygulanabilirlik Bildirgesi üretilmesi,

e) Bir bilgi güvenliği risk işleme planının formüle edilmesi,

f) Bilgi güvenliği risk işleme planına dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin kabulü,

Üniversitemiz, bilgi güvenliği risk işleme süreci ile ilgili yazılı bilgileri KSP.KYS-PR-002 Kayıtların Kontrolü Prosedürüne uygun olarak muhafaza etmektedir.

6.2. Bilgi Güvenliği Amaçları ve Amaçları Başarmak için Planlama

Kurumumuz ilgili fonksiyon ve seviyelerinde kalite amaçları KSP.KYS.FR.019 Kalite Amaç Planlarını oluşturulmuştur. Kalite amaçları yıllık yapılan Yönetimi Gözden Geçirme toplantıları ile gözden geçirilmektedir.

Bilgi Güvenliği amaçları:

a) Bilgi Güvenliği politikası ile uyumlu olmalı,

b) Ölçülebilir olmalı(uygulanabilirse),

c) Uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme ve risk işlemenin sonuçlarını dikkate almalı,

d) Duyurulmalı,

e) Uygun şekilde güncellenmelidir.

Üniversitemiz bilgi güvenliği amaçları ile ilgili yazılı bilgileri KSP.KYS-PR-002 Kayıtların Kontrolü Prosedürüne uygun olarak muhafaza etmektedir.

Bilgi Güvenliği amaçlarının nasıl başarılacağı aşağıdaki unsurlar planlanarak belirlenmiştir.

a) Ne yapılacağı,

b) Hangi kaynakların gerekeceği,

c) Kimin sorumlu olacağı,

d) Ne zaman tamamlanacağı,

e) Sonuçların nasıl değerlendirileceği.

Referans: KSP.KYS-PR-002 Kayıtların Kontrolü Prosedürü

KSP.KYS.FR.019 Kalite Amaç Planları

7. DESTEK

7.1.Kaynaklar

Kapadokya Üniversitesi Mütevelli Heyeti, Bilgi Güvenliği Yönetim Sistemi'nin uygulanması, sürdürülmesi ve etkinliğinin sürekli iyileştirilmesi için ihtiyaç duyulan kaynakları tayin etmekte ve sağlamaktadır. Mütevelli Heyetimiz aşağıdaki konuları yaptığı toplantılarda ve Yönetimi Gözden Geçirme Toplantısında değerlendirmektedir.

a) Var olan iç kaynakların yeteneklerini ve kısıtlamalarını,
b) Dış Tedarikçilerden neyin tedarik edileceğini,

İnsan kaynaklı tehditler için BGYS-PR-010 İnsan Kaynakları Güvenliği Prosedürü' ne uygun olarak hareket edilmektedir.

7.2. Yeterlilik

Kapadokya Üniversitesi bünyesinde görevin gerektirdiği öğrenim, eğitim, beceri, tecrübe ve yeterliliğe sahip personelin temin edilmesi esastır.

a) Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişilerin gerekli yeterliliklerinin belirlenmesi,
b) Uygun öğretim, eğitim veya tecrübe temelinde bu kişilerin yeterliliklerinin temin edilmesi,
c) Uygun olduğu durumlarda, gerekli yeterliliğin sağlanması için girişimde bulunulması ve bu girişimlerin etkinliğinin değerlendirilmesi,
d) Yeterliliğin delili olarak uygun yazılı bilgilerin muhafaza edilmesi.

Üniversitemizde, Öğretim Elemanı ve Öğrencilerimizin Bilgi Güvenliği Yönetim Sistemine katkılarının arttırılması amacıyla, gereken eğitimlerin tespit edilmesi ve verilmesine ilişkin çalışmalar Sürekli Eğitim Uygulama ve Araştırma Merkezi (SEM) tarafından organize edilmektedir.

Tutulan kayıtlar KSP.KYS.PR.001 Kayıtların Kontrolü Prosedürüne uygun olarak muhafaza edilmektedir.

7.3.Farkındalık;

Üniversitemiz kontrolü dâhilinde görev yapan kişiler aşağıdakilerin farkında olmalıdır:

a) Bilgi güvenliği politikası,

b) İyileştirilmiş bilgi güvenliği performansının faydaları da dâhil bilgi güvenliği yönetim sisteminin etkinliğine yaptıkları katkı,

c) Bilgi güvenliği yönetim sistemi şartlarına uyum sağlamamanın sonuçları.

Üniversitemizde, görev yapan Öğretim Elemanı ve İdari Personeller için (İK.FR.024 Eğitim Talep Formu) kurulan Bilgi Güvenliği Yönetim Sisteminin farkındalığını sağlamak için İnsan Kaynakları ve Sürekli Eğitim Uygulama ve Araştırma Merkezi tarafından eğitimler organize edilmektedir. Üniversitemizde bulunan öğrencilerimizin talep etmesi durumunda (SEM.FR.002 Eğitim Başvuru Formu) Bilgi Güvenliği Yönetim Sistemi konusunda bilgilendirme amaçlı eğitimler de organize edilmektedir.

Referans: KSP.KYS.PR.001 Kayıtların Kontrolü Prosedürüne
BGYS-PR-010 İnsan Kaynakları Güvenliği Prosedürü
YN -010 Öğretim Elemanı Görevlendirme Yönergesi
İK.TL-001 İnsan Kaynakları Personel İşleri Talimatı
İK.TL-002 Atama Talimatı
SEM.FR.002 Eğitim Başvuru Formu
SEM.FR.001 Eğitim Katılımcı Listesi
SEM.FR.004 Eğitim Geliştirme Formu
SEM.FR.012 Online Eğitim Talep Formu
İK.FR.001 Personel Eğitim Etkinliği Değerlendirme Formu
İK.FR.002 Eğitim Sonuç Raporu
İK.FR.003 Personel Eğitim Takip Kartı
İK.FR.004 Yıllık Eğitim Programı
İK.FR.011 Personel Bilgi Güncelleme Formu
İK.FR.018 Öğretim Görevlisi Kalifikasyon Bilgi Formu
İK.FR.024 Eğitim Talep Formu

7.4. İletişim

Kuruluş aşağıdakileri içeren bilgi güvenliği yönetim sistemi ile ilgili dâhili ve harici iletişim ihtiyaçlarını belirlemelidir:

a) İletişimin konusu,

b) Ne zaman iletişim kurulacağı,

c) Kiminle iletişim kurulacağı,

d) Kimin iletişim kuracağı,

e) İletişimin hangi süreçten etkileneceği.

Üniversitemizde, iletişimin hangi şartlarda kiminle, neyle ilgili, ne zaman, nasıl, kimin iletişim kuracağına dair, iç ve dış iletişimleri **Bİ.FR-004 İletişim Formu** üzerinden oluşturulmuştur ve uygulanmaktadır.

7.5. Yazılı Bilgiler

7.5.1. Genel

Üniversitemizde Bilgi Güvenliği yönetim sistemi aşağıdakileri içermektedir.

a) TS EN ISO 27001 Standardında istenen dokümante edilmiş bilgiyi,

b) Kuruluşumuz tarafından, Bilgi Güvenliği yönetim sisteminin etkinliğini artırmak için belirlenen dokümante edilmiş bilgiyi.

Bilgi Güvenliği Yönetim Sistemimizin yazılı bilgilerin boyutu aşağıdaki maddeleri dikkate alınarak oluşturulmuştur. Bunlar;

1. Kuruluşun büyüklüğü ve faaliyetlerinin, süreçlerinin, ürünlerinin ve hizmetlerinin türleri,
2. Süreçlerin ve etkileşimlerinin karmaşıklığı
3. Kişilerin yeterliliği.

Üniversitemizde, Bilgi Güvenliği Yönetim Sistemi dokümanları KSP.KYS.PR.001 Dokümanların Kontrolü Prosedüründe tanımlanmıştır.

7.5.2. Oluşturma ve Güncelleme

Üniversitemiz; dokümante edilmiş bilgileri oluştururken ve güncellerken aşağıdakileri uygun şekilde KSP.KYS.PR.001 Dokümanların Kontrolü Prosedüründe ile güvence altına almıştır:

a) Tanımlama ve açıklama (örneğin, bir başlık, tarih, yazar veya referans numarası),

b) Biçim (örneğin, dil, yazılım sürümü, grafikler) ve ortam (örneğin, kâğıt, elektronik),

c) Uygunluk ve doğruluğun gözden geçirilmesi ve onaylanması.

7.5.3. Yazılı Bilgilerin Kontrolü

7.5.3.1. Bilgi Güvenliği yönetim sistemi ve bu standart tarafından istenen dokümante edilmiş bilgi, aşağıdakileri güvence altına almak için kontrol edilmektedir.

a) Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olmasın (BGYS-PR-12 Erişim Kontrolü Prosedürü),

b) Doğru bir şekilde korunması (örneğin, gizliliğin yok olması, uygun olmayan kullanım veya bütünlüğün kaybolması).

7.5.3.2. Dokümante edilmiş bilginin kontrolü için kuruluşumuz aşağıdaki faaliyetlerden uygulanabilir olanları KSP.KYS.PR.001 Dokümanların Kontrolü Prosedürü ve KSP.KYS.PR.001 Kayıtların Kontrolü Prosedürüne ile belirlemiştir:

a) Dağıtım, erişim, kullanım ve tekrar kullanım (BGYS-PR-012 Erişim Kontrolü Prosedürü' ne ve BGYS-PR-015 Haberleşme Güvenliği Prosedürüne göre yapılmaktadır)

b) Okunaklılığın korunması da dahil olmak üzere saklama ve koruma,

c) Değişikliklerin kontrolü (örneğin, sürüm kontrolü vb.),

d) Muhafaza etme ve yok etme.

Üniversitemizde çıktı olarak dokümante edilmiş kayıtlar;

- Öğretim Programı kapsamındaki dokümante edilmiş bilgiler bölümlerde muhafaza edilmektedir.
- İdari bölümlerde dokümante edilmiş bilgiler kendi bölümlerinde muhafaza edilmektedir.

- Bölümlerde tutulan kayıtların süresi dolduğunda Kütüphane ve Dokümantasyon Dairesine aktarılmaktadır. Dokümante edilmiş bilgiler belirlenen imha süresine kadar burada muhafaza edilmektedir.

Üniversitemizin faaliyetlerini etkileyen iç kaynaklı dokümante edilmiş bilgilerin takibi KSP.FR.001 Doküman Revizyon Takip Formu ve KSP.FR.002 Doküman Değişiklik Talep Formu ile Bilgi Güvenliği ve Stratejik Planlama Dairesi tarafından takip edilir.

Üniversitemizin faaliyetlerini etkileyen dış kaynaklı dokümante edilmiş bilgilerin takibi bölüm sorumluları tarafından KSP.FR.21 Dış Kaynaklı Doküman Takip Listesi takip edilir.

Varlıkların kontrolü BGYS-PR-011 Varlık Yönetimi Prosedürüne uygun olarak yapılmaktadır. Varlık envanteri Bilgi işlem Bölümü tarafından oluşturulan program üzerinden yürütülmektedir.

Varlıkların değişen fiziksel alanlara ve çevresel güvenlikleri BGYS-PR-013 Fiziksel Alanlar ve Çevresel Güvenliği Prosedürü' nde tanımlanmıştır.

Güvenlik gereksinimleri BGYS-PR-016 Sistem Temini, Geliştirme ve Bakım Prosedürü' nde tanımlanmıştır.

Bilgi güvenliği ile ilgili ihlal ve iyileştirmeler BGYS-PR-018 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü' nde tanımlanmıştır.

Referans:

KSP.KYS.PR.001 Dokümanların Kontrolü Prosedürü

KSP.KYS.PR.002 Kayıtların Kontrolü Prosedürüne

BGYS-PR-011 Varlık Yönetimi Prosedürüne

BGYS-PR-012 Erişim Kontrolü Prosedürü

BGYS-PR-013 Fiziksel Alanlar ve Çevresel Güvenliği Prosedürü

BGYS-PR-015 Haberleşme Güvenliği Prosedürüne

BGYS-PR-016 Sistem Temini, Geliştirme ve Bakım Prosedürü

BGYS-PR-018 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü

KSP.FR.001 Doküman Revizyon Takip Formu

KSP.FR.002 Doküman Değişiklik Talep Formu

KSP.FR.21 Dış Kaynaklı Doküman Takip Listesi

KD.TL.001 Arşiv Talimatı

KD.TL.002 İletişim ve Yazışma Talimatı

8. EĞİTİM VE ÖĞRENİM (OPERASYONEL)

8.1. Eğitim ve Öğrenimin Planlaması ve Kontrolü

Kapadokya Üniversitesi bünyesinde, öğrencilere, akademisyenlere ve idari birim personeline sunulan hizmetler; 2547 sayılı Yükseköğretim Kanunu, Vakıf Yükseköğretim Kurumları Yönetmeliği ve 124 sayılı Yükseköğretim Üst Kuruluşları ile Yükseköğretim Kurumlarının İdari Teşkilatı Hakkında Kanun Hükmünde Kararname hükümlerine uygun olarak tespit edilen akademik ve idari birimler tarafından gerçekleştirilir.

Üniversitemizde eğitim öğretim hizmetlerinin etkin bir şekilde gerçekleştirilebilmesi için, bu hizmetler sunulmadan önce gerekli planlama ve hazırlık faaliyetlerinin gerçekleştirilir.

Eğitim öğretim hizmetlerinin planlanması; eğitim verilecek bölüm ve programlar, bölüm ve programların kontenjanları, tüm birimler için akademik takvim hazırlanması, kayıtların yapılması, derslerin öğretim elemanlarının belirlenmesi, eğitim kabulü için sınav programlarının hazırlanması işlemlerini kapsar. Eğitim ve Öğrenimin şartlarına uygunluğu sağlamak için ihtiyaç duyulan kaynakların tayin edilmiştir.

Eğitim verilen bölüm ve programlar iç değerlendirmesi öğrencilerin başarı seviyesini gösteren sınavların içeriği ve sonuçları değerlendirilmektedir. Dış değerlendirme olarak üniversitemizin bağlı olduğu YÖK tarafından yapılan değerlendirme ve kontroller ile yapılmaktadır. Uygulama ve Araştırma Merkezimize bağlı bölümlerin denetimleri ise yetki alınan kurum/kuruluşlar tarafından yapılan denetimler ile sağlanmaktadır.

Eğitim öğretim hizmetlerinin planlanması ile ilgili metotlar, ilgili yasal mevzuat şartları da dikkate alınarak belirlenmiş ve Bilgi Güvenliği Yönetim Sistem dokümantasyonunda tanımlanmıştır.

Referans: EPY.TL.061 Eğitim Faaliyetlerinin Planlanması ve Organizasyonu Talimatı

EYP.FR.026 Program Başarı Analiz Formu

8.2. Bilgi Güvenliği Risk Değerlendirme

Üniversitemiz, aşağıda belirtilen kriterleri de dikkate alarak, bilgi güvenliği risk değerlendirmelerini planlanan aralıklarda veya önemli değişiklikler önerildiğinde veya meydana geldiğinde gerçekleştirmelidir.

a) Aşağıdakileri içeren bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi:

1. Risk kabul kriterleri,
2. Bilgi güvenliği risk değerlendirmesi yapılması için kriterler,

Üniversitemiz, bilgi güvenliği risk değerlendirmesinin sonuçlarına dair yazılı bilgileri KSP.KYS.PR.002 Kayıtların Kontrolü Prosedürüne uygun olarak muhafaza etmektedir.

8.3. Bilgi Güvenliği Risk İşleme

Üniversitemiz, bilgi güvenliği KSP.BGYS.FR.029 Risk İşleme Planı uygulamaktadır. Çalışmalar BGYS.PR.021 BGYS Risk Analiz Prosedürü' nde tanımlanmıştır. Bilgi güvenliği risk işlemesinin sonuçlarına ait yazılı bilgileri KSP.KYS.PR.002 Kayıtların Kontrolü Prosedürüne uygun olarak muhafaza etmektedir.

Referans: BGYS.PR.021 BGYS Risk Analiz Prosedürü

KSP.KYS.PR.002 Kayıtların Kontrolü Prosedürü

KSP.BGYS.FR.029 Risk İşleme Planı

9. PERFORMANS DEĞERLENDİRME

9.1. İzleme, Ölçme, Analiz ve Değerlendirme

Bilgi Güvenliği Yönetim Sisteminin etkinliğini ve uygunluğunu değerlendirmek ve sistemi sürekli iyileştirmek amacına yönelik olarak neler yapılabileceğini tespit etmek için veriler toplanır ve analiz edilir. Veriler yapılan anketlerden ve/veya gelen şikâyet ve önerilerden elde edilir.

Üniversitemiz aşağıdakileri konuları belirlemiştir.

a) Bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere neyin izlenmesi ve ölçülmesinin gerekli olduğu,

b) Geçerli sonuçları temin etmek için, uygun izleme, ölçme, analiz ve değerlendirme yöntemleri,

Seçilen yöntemlerin geçerli kabul edilebilmesi için karşılaştırılabilir ve tekrar üretilebilir sonuçlar üretmesi gerekmektedir.

c) İzleme ve ölçmenin ne zaman yapılacağı,

d) İzlemeyi ve ölçmeyi kimin yapacağı,

e) İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği,

f) Bu sonuçları kimin analiz edeceği ve değerlendireceği.

Üniversitemiz, izleme ve ölçme sonuçlarına dair delil olarak uygun yazılı bilgileri muhafaza edecek yapıyı oluşturmuştur.

Bilgi Güvenliği Yönetim Sistemi dokümantasyonu, mevzuatın zorunlu kıldığı veya Bilgi Güvenliği Yönetim Sistemi için gerek görülen raporlar ile bunların hazırlanma ve yayınlanmasına ilişkin metotları tanımlamaktadır.

Referans: KSP.TL.002 Veri Analizi Talimatı

9.2. İç Tetkik

Bilgi Güvenliği yönetim sisteminin, ilgili standart, mevzuat ve Üniversitemiz tarafından oluşturulan Bilgi Güvenliği yönetim sisteminin şartlarına uygunluğunu ve sistemin etkin olarak uygulandığını ve sürdürüldüğünü teyit etmek için planlı aralıklarla iç denetim yapılır. Bu denetimler Kapadokya Üniversitemizin yönetimi tarafından atanmış, bağımsız, tarafsız ve eğitilmiş personel tarafından gerçekleştirilir.

Kapadokya Üniversitemiz, bilgi güvenliği yönetim sisteminin, aşağıdaki hususları yerine getirip getirmediği konusunda bilgi elde etmek için planlanan aralıklarda iç tetkikler gerçekleştirmektedir:

a) Aşağıdakilerle uyumlu olup olmadığı;

1. Bilgi güvenliği yönetim sistemi ile ilgili olarak kuruluşun kendi şartları,
2. Bu standardın şartları,

b) Etkin bir şekilde uygulanması ve sürdürülmesi.

Kuruluş aşağıdakileri gerçekleştirmelidir:

c) Sıklık, yöntemler, sorumluluklar, gereksinimleri planlama ve raporlama da dâhil olmak üzere bir tetkik programının/programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi. Tetkik programı/programları ilgili süreçlerin önemini ve önceki tetkiklerin sonuçlarını dikkate almalıdır,

d) Her bir tetkik için tetkik kriterlerinin ve kapsamın tanımlanması,

e) Tetkik sürecinin tarafsızlığı ve objektifliğini temin edecek şekilde tetkikçilerin seçimi ve tetkiklerin yürütülmesi,

f) Tetkik sonuçlarının uygun yönetim kademesine raporlanmasının temin edilmesi,

g) Tetkik programı/programları ve tetkik sonuçlarının delil teşkil eden yazılı bilgilerinin muhafaza edilmesi.

Denetleme ve değerlendirme faaliyetleri İç Tetkik Prosedürü dikkate alınarak yapılan planlamalar doğrultusunda gerçekleştirilir. Denetleme sonrası takip faaliyetleri sürdürülerek çalışmaların amaca ulaşması sağlanır.

Nihai hedef, ulaşılan Bilgi Güvenliği düzeyinde geriye dönüşleri önlemek ve yeni Bilgi Güvenliği geliştirme faaliyetlerini ortaya çıkarmaktır.

Referans: KSP.KYS.PR.003 İç Tetkik Prosedürü
YNG-012 Öğrenci Rehberliği ve Danışmanlığı Yönergesi
KİH.TL.007 Öğrenci Şikayetleri ve Memnuniyeti Değerlendirme Talimatı

9.3. Yönetimin Gözden Geçirmesi

Kapadokya Üniversitesinde, Bilgi Güvenliği yönetim sisteminin uygunluğunun, yeterliliğinin ve etkinliğinin sürekliliğini sağlamak amacıyla planlanmış aralıklarla Yönetim Gözden Geçirmesi faaliyetleri yürütülür.

Üst yönetim bilgi güvenliği yönetim sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla gözden geçirmelidir. Yönetimin gözden geçirmesi aşağıdakileri ele alınmaktadır:

a) Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu,
b) Bilgi güvenliği yönetim sistemini ilgilendiren dış ve iç konulardaki değişiklikler,
c) Aşağıdakiler deki gelişmeler dâhil bilgi güvenliği performansına dair geri bildirim:
    1. Uygunsuzluklar ve düzeltici faaliyetler,
    2. İzleme ve ölçme sonuçları,
    3. İç ve Dış Tetkik sonuçları,
    4. Bilgi güvenliği amaçlarının yerine getirilmesi,
d) İlgili taraflardan geri bildirimler,
e) Risk değerlendirme sonuçları ve risk işleme planının durumu,
f) Sürekli iyileştirme için fırsatlar.

Yönetimin gözden geçirmesi çıktıları, sürekli iyileştirme fırsatlarına ve bilgi güvenliği yönetim sisteminde gerekli olan değişiklikler için tüm ihtiyaçlara dair kararları içermelidir.

Üniversitemiz, yönetimin gözden geçirmesinin sonuçlarının delili olarak KSP.FR.007 Toplantı Tutanak Formu ile kayıt altına almaktadır. Yazılı bilgiler KSP.KYS.PR.002 Kayıtların

Kontrolü Prosedürüne uygun olarak muhafaza etmektedir. Yönetim Gözden Geçirmesi süreçlerine ilişkin esaslar Kalite Komisyonu Yönergesinde tanımlanmıştır.

10. İYİLEŞTİRME

10.1. Uygunsuzluk ve Düzeltici Faaliyet

Kapadokya Üniversitesi, uygunsuzlukların nedenini gidermek ve tekrarını önlemek için gerekli tedbirleri KSP.KYS.PR.004 Uygun Olmayan Hizmetin Kontrolü Prosedürüne göre almaktadır.

Karşılaşılan uygunsuzluğun sebebini ortadan kaldıracak "düzeltici faaliyet" belirlenir ve uygulanır. Bilgi Güvenliğine yönelik ihlal olaylarında BGYS-PR-018 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü' ne göre hareket edilir. Bu sistemde, ilgili prosedürler doğrultusunda tespit edilen uygunsuzluklar ele alınmakta; hizmetler ve Bilgi Güvenliği Yönetim Sistemi ile ilgili olan uygunsuzlukların sebepleri detaylı bir şekilde araştırılmakta; bu uygunsuzlukların sebeplerini yok etmek için gerekli olan düzeltici faaliyetler tamamlanmakta ve düzeltici faaliyetlerin gerçekleşip gerçekleşmediğinin kontrolü yapılmaktadır. Düzeltici faaliyetler; bu konuda oluşturulan düzeltici faaliyet formuna uygunsuzluk açıkça tarif edilecek şekilde yazılır. Açılan düzeltici faaliyetlerin en geç belirtilen bitiş süresinde ilgili sorumlusu veya onun delege ettiği kişiler tarafından gözden geçirilir.

Referans: KSP.KYS.PR.004 Uygun Olmayan Hizmetin Kontrolü Prosedürü

KSP.KYS.PR.005 Düzeltici İşlem Prosedürü

BGYS-PR-018 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü

10.2. Sürekli İyileştirme

Bilgi Güvenliği Yönetim sisteminin etkinliği, Bilgi Güvenliği Politikasının ve amaçların bütün birimlerde anlaşılıp uygulanmasının sağlanması, iç ve dış tetkik sonuçlarının analizi, düzeltici faaliyetlerin etkin bir şekilde uygulanması ve yönetimin gözden geçirmesi yoluyla iyileştirilmektedir.