KAPADOKYA ÜNİVERSİTESİ

Akıl - Ahlak - Adalet - Adap

BİLGİ GÜVENLİĞİ EL KİTABI

Doküman No: BGEK-001
Yayın Tarihi: Aralık 2017
Revizyon No: 01
Revizyon Tarihi: Mart 2022

İÇİNDEKİLER

ÖNSÖZ 3

REVİZYON LİSTESİ 4

DAĞITIM LİSTESİ 5

ONAY 6

A. GENEL 7

B. KALİTE EL KİTABI REVİZYON VE DAĞITIMI 7

C. ÜNİVERSİTEMİZİN TANITIMI: 7

BİLGİ GÜVENLİĞİ POLİTİKALARIMIZ 9

1. AMAÇ 10

2. KAPSAM 10

3. HARİÇ TUTULAN STANDART MADDELERİ 10

4. ÜNİVERSİTEMİZİN BAĞLAMI 11

4.1. Kuruluş ve Bağlamının Anlaşılması: 11

4.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması 12

4.3. Bilgi Güvenliği Yönetim Sistemi Kapsamının Belirlenmesi 12

4.4. Bilgi Güvenliği Yönetim Sistemi ve Prosesleri 13

5. LİDERLİK 13

5.1. Liderlik ve Bağımlılık 13

5.2. Politika 14

5.3. Kurumsal Görev, Sorumluluklar ve Yetkiler 14

6. PLANLAMA 15

6.1. Risk ve Fırsatları Ele Alan Faaliyetler 15

6.1.2. Bilgi Güvenliği Risk Değerlendirme 15

6.1.3. Bilgi Güvenliği Risk İşleme 16

6.2. Bilgi Güvenliği Amaçları ve Amaçları Başarmak için Planlama 17

7. DESTEK 18

7.1. Kaynaklar 18

7.2. Yeterlilik 18

7.4. İletişim 20

7.5. Yazılı Bilgiler 20

8.1. Eğitim ve Öğrenimin Planlaması ve Kontrolü 23

8.2. Bilgi Güvenliği Risk Değerlendirme 24

8.3. Bilgi Güvenliği Risk İşleme 24

9. PERFORMANS DEĞERLENDİRME 25

9.1. İzleme, Ölçme, Analiz ve Değerlendirme 25

9.2. İç Tetkik 26

9.3. Yönetimin Gözden Geçirmesi 27

10.İYİLEŞTİRME 27

10.1. Uygunsuzluk ve Düzeltici Faaliyet 28

10.2. Sürekli İyileştirme 28

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
BGEK-001	01	Mart 2022	Yıllık gözden geçirme	Bilgehan KAMBER

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: Bİ.PR.013 BGYS Uyum Prosedürü

A. GENEL

Bilgi Güvenliği El Kitabı'nın revizyonu ve dağıtımı Bilgi İşlem Dairesinin sorumluluğundadır. Revizyon kayıtları Kalite ve Stratejik Planlama Dairesi tarafından tutulur.

Birimlerin Revizyon istekleri **KSP.PR.002 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 el kitabının 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 TS EN ISO 27001 Bilgi Güvenliği kapsamında, **Bİ.PR.001 Bilgi Güvenliği Politikaları Prosedürü** uygun olarak hazırlanır. Hazırlanan politikalar aşağıdaki gibi listelenmiştir.

- Bilgi Güvenliği Politikası,
- Erişim Kontrol Politikası,
- Güvenli Geliştirme Politikası,
- Güvenlik Politikası,
- Kişisel Verilerin Korunması ve İşlenmesi Politikası
- Mobil Cihaz Politikası
- Tedarikçi İlişkileri Politikası,
- Temiz Masa Temiz Ekran Politikası,

Referans: 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,
Bİ.PL.006 Kişisel-Verilerin-Korunması-ve-İşlenmesi-Politikası
Bİ.BGP.007 Mobil Cihaz Politikası
Bİ.BGP.008 Güvenlik 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 Mustafaşa, Ürgüp Nevşehir adresinde faaliyette bulunan Kapadokya üniversitesinin tüm eğitim, öğretim ve destek hizmetleri süreçlerini 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 bilgi güvenliği yönetim sisteminin istenen sonuçlarını elde etme yeteneğini etkileyecek iç ve dış hususları belirlemiştir. Bu faktörler kurumun faaliyet kapsamı, lokasyonu gibi majör değişikliklerde gözden geçirilmektedir.

İç hususlar; misyon, vizyon, hedefler, değerler, politikalar, teknolojik altyapı, mali kaynaklar, teşkilat yapısı, öncelikli alanlar, akreditasyon, diploma, nitelikli eğitim ve toplumsal katkı ile paydaşlarımızın beklentileridir.

Dış hususlar; YÖK mevzuatı, YÖKAK mevzuatı ve ölçütleri, Akreditasyonlar, nitelikli kadro, inovasyon odaklı teknoloji, uluslararası rekabet ve konumdur.

KÜN bünyesinde her beş yılda bir Stratejik Plan Hazırlama Kurulu tarafından kurumun güçlü ve zayıf yönleri ile fırsat ve tehditlerinin belirlenebilmesi amacı ile hem iç paydaş hem de dış paydaş gözünden SWOT analizi gerçekleştirilir. SWOT analizi ekseninde kurumun güçlü yönlerinin etkinliğinin arttırılması, zayıf yönlerinin iyileştirilmesi, olası tehditlerin bertarafı ve fırsatların kuruma kazandıracağı stratejik amaçlar doğrultusunda temel ilke ve politikalarını, önceliklerini ve bunlara ulaşmak için izlenecek yol ve yöntemler ile kaynak dağılımını düzenleyen orta vadeli planlamayı içeren beş yıllık Stratejik Plan düzenlenmektedir.

Bununla birlikte BGYS için SWOT analizi **Bİ.FR.024 SWOT Analiz Formu** ile yapılmıştır.

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

4.2. İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

ISO 27001 kapsamında öğrenciler, akademik ve idari birimler, tedarikçiler, tüm özel ve kamu kuruluşları ve dış ziyaretçiler ilgili taraflar olarak belirlenmiştir. Bilgi İşlem Daire Başkanlığı ana fonksiyonu belirli bir zaman periyodu içerisinde iç ve dış paydaşlara yönelik hizmetleri ve uygulamaya konulan Bilgi Güvenliği Yönetim Sisteminin kullanılan bütün yazılım ve diğer hizmet sunumu faaliyetlerini kapsamaktadır. Hizmet kalitesine etkisi bulunabilecek tüm ISO 27001 standart maddeleri, Bilgi Güvenliği Yönetim Sistemi kapsamına alınmıştır.

Üniversitenin ilgili tarafların **Bİ.FR.025 İlgili Tarafların İhtiyaç ve Beklentileri Formu** ile belirlenmiştir.

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 bölümler bazında hazırlanan proseslerde tanımlanmıştır. 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 (**Bİ.BGP.001 Bilgi Güvenliği Politikası).** 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

Bilgi güvenliği politikaların Üniversite personeli tarafından bilinirlik ve anlaşılırlığını sağlamak için "Bilgi Güvenliği Yönetim Sistemi El Kitabı" hazırlanmış ve verilen eğitimlerle anlaşılması sağlanmıştır. Bilgi Güvenliği politikası internet kalite portalı üzerinden paylaşılarak duyurulmaktadır (http://kalite.kapadokya.edu.tr/Bilgi-Guvenligi-Politikalari). Bilgi Güvenliği Yönetim Sistemleri Politikalarının uygunluğunun sürekliliği, YGG toplantılarında gözden geçirilerek etkin uygulanması açısından gerekli kararlar alınmaktadır.

5.3. Kurumsal Görev, Sorumluluklar ve Yetkiler

Üniversiteye ait organizasyon şeması entegre kalite yönetim sistemi kapsamında tanımlanmış ve yayınlanmıştır. Bilgi güvenliği yönetim sistemi çalışmalarını Bilgi İşlem Dairesi ve Kalite ve Stratejik Planlama Dairesi ile koordineli şekilde yürütecektir. (Organizasyon Şeması)

Bilgi güvenliği operasyonu ve uygulamasının başlatılması ve kontrol edilmesi **Bİ.PR.002. Bilgi Güvenliği Organizasyon Prosedürü** ile açıklanmıştır.

Kurumsal görev, yetki ve sorumlulukların belirlenmesi amacıyla görev tanımları oluşturulmuştur. Birimler içerisinde görevli olan tüm personellerin sorumlulukları, yetkileri ve yeterlilikleri belirlenmiş olup kalite portalı üzerinden tüm birimlerin erişimine açılmıştır.

6. PLANLAMA

6.1. Risk ve Fırsatları Ele Alan Faaliyetler

6.1.1. Genel

Kapadokya Üniversitesi yönetim sistemleri risk ve fırsatların belirlenmesi, süreçlere bağlı olarak yürütülmektedir. Riskler proses bazında değerlendirilerek **Bİ.FR.008 Risk Analiz Formu** ile takip edilmektedir. İlgili riskler **Bİ.FR.021 Risk İşleme Planına** kaydedilir. Risk ve fırsatlar yılda bir kere Yönetim Gözden Geçirme Toplantıları ve yılda 1 kere iç denetimler ile izlenmekte ve gerektiğinde güncellenmektedir.

Üniversite bünyesinde her sürece ait risk analizi gerçekleştirilmektedir. Riskin ne olduğu ve alınacak olan önlemler tanımlanarak, riskin yaratacağı etki ve riskin gerçekleşme olasılığı çarpılarak risk derecesi hesaplanmaktadır. Risk analiz yöntemi **Bİ.PR.014 BGYS Risk Analizi Prosedüründe** detaylı olarak açıklanmıştır.

6.1.2. Bilgi Güvenliği Risk Değerlendirme

Üniversitemiz, akademik ve idari birimlerinde Bilgi Güvenliğini sağlamak ve geliştirmek için **Bİ.PR.014 BGYS Risk Analizi 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 **Bİ.PR.014 BGYS Risk Analizi Prosedürünün** 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

Bilgi Güvenliğini risk işleme için **Bİ.PR.014 BGYS Risk Analizi Prosedürü** oluşturulmuş

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.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 **Bİ.FR.007 Bilgi Güvenliği Amaç ve Hedef Planları** oluşturulmuştur. Bilgi Güvenliği amaç ve hedefleri yıllık yapılan Yönetimi Gözden Geçirme toplantıları ile gözden geçirilmektedir. Bu yolla BGYS performansının ölçümü yapılmaktadır.

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.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.

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,

Kapadokya Üniversitesi Yönetim Sistemlerinin uygulanması, sürdürülmesi, etkinliğinin sürekli iyileştirilmesi, öğrenci ihtiyaç ve beklentilerinin yerine getirilmesi ve öğrenci memnuniyetinin arttırılmasına yönelik gerekli kaynak ihtiyaçlarını belirlemiş olup temin etmektedir.

Mali kaynaklar bütçe disiplini içerisinde yönetilmektedir. Bütçe uygulamalarının tüm süreçleri Bütçe Hazırlama Talimatında tanımlanmıştır. Her akademik yıl başında tüm birimlerden yürütme ve yatırım ihtiyaçları talep edilmekte, mevcut kaynaklar bu ihtiyaçlara göre planlanmaktadır. Yatırım ve harcamalar önceliklendirilmektedir.

Kapadokya Üniversitesi insan kaynakları yönetim sistemi geliştirme çalışmaları kapsamında personel yönetimi yazılımı temin edilmiş ve süreçler bu yazılımla idare edilir hale getirilmiştir. Bu kapsamda Üniversite bünyesinde görev alan akademik ve idari personelin tamamının özlük işleri ve personel bazında gerekli eğitimlerin geçerlik süreleri takip edilmektedir. Personelin performanslarını ölçmeye yönelik süreçler kalite sistemi içerisinde "**Performans Değerlendirme Yönergesi**" ve "**Akademik Personel Performans Değerlendirme Yönergesi**" ile tanımlanmıştır.

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 İnsan Kaynakları Dairesi tarafından organize 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.

İnsan Kaynakları Dairesi tarafından **İK.FR.004 Yıllık Eğitim Programı** ile takip edilmekte ve planlanmaktadır.

Referans: BGYS-PR-003 İnsan Kaynakları Güvenliği Prosedürü
SEM.FR.001 Eğitim Katılımcı Listesi
SEM.FR.002 Eğitim Başvuru Formu
SEM.FR.004 Eğitim Geliştirme Formu
İK.FR.001 Personel Eğitim Etkinliği Değerlendirme Formu
İK.FR.002 Eğitim Sonuç Raporu
İK.FR.004 Yıllık Eğitim Programı
İK.FR.024 Eğitim Talep Formu

7.4. İletişim

Üst yönetim hizmetler ve Bilgi Güvenliği yönetim sisteminin yürütülmesi için gerekli olan iç ve dış iletişimi eksiksiz olarak yerine getirilmesini güvence altına alabilmek amacıyla;

- İç ve dış yazışmalar,
- Elektronik posta,
- Telefon, faks,
- Hizmet içi eğitimler,
- YGG toplantıları,
- Yüz yüze görüşmeler,
- Uzaktan Toplantılar
- EBYS,
- Üniversite web siteleri,

gibi yöntemleri kullanmaktadır.

Üniversitemizde, iletişimin hangi şartlarda kiminle, neyle ilgili, ne zaman, nasıl, kimin iletişim kuracağına dair, iç ve dış iletişimleri **KSP.FR.025 İletişim Tablosu** üzerinden oluşturulmuştur ve uygulanmaktadır.

7.5. Yazılı Bilgiler

7.5.1. Genel

Üniversite süreçlerinin etkin ve verimli bir şekilde yürütülmesini sağlamak amacıyla Bilgi Güvenliği yönetim sisteminde yer alan temel dokümanlardan yararlanılmıştır. Oluşturulan tüm dokümanlar KSP.LS.004 Ana Doküman Listesinde tanımlanmıştır. Kayırların oluşturulmasında KSP.PR.002 Dokümantasyon Prosedürüne uygun hareket edilir.

- Konular hakkındaki en genel yaklaşım ve prensipleri belirlemek için **politikalar** hazırlanmıştır.
- Yönetsel ve kapsamlı işlemlerin tarif edilmesi için prosedürler yazılmıştır. **Prosedür** bir işi Kimin, Ne, Nasıl, Nerede, Niçin ve Ne Zaman yaptığını açıklamaktadır.

- İş ve işlemlerin girdi, çıktı, kaynak, kontrol kriteri, performans kriteri, risk ve fırsatlarını belirlemek amacıyla **prosesler** oluşturulmuştur.

- Süreçler içerisinde kullanılan formların standart hale getirilmesi için **formlar** hazırlanmıştır.
- Üniversite içerisindeki yetki ve sorumlulukların net bir şekilde belirlenmesi adına **görev tanımları** oluşturulmuştur.
- Talimatlar, kılavuzlar, listeler,

Tüm dokümanlar Bilgi Güvenliği yönetim sistemi kapsamında, alanında uzman kişiler tarafından hazırlanmış olup, **kalite.kapadokya.edu.tr** adresinde yayınlanarak tüm personelin erişimine sunulmuştur.

7.5.2. Oluşturma ve Güncelleme

Üniversitemiz; dokümante edilmiş bilgileri oluştururken ve güncellerken aşağıdakileri uygun şekilde **KSP.PR.002 Dokümantasyon Prosedürüne** 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

Tüm personel, kullandıkları dokümanları yaptıkları işe uygunluk açısından sürekli olarak gözden geçirmektedir. Zaman içerisinde faaliyetlerdeki değişiklikler ve gelişmeler nedeniyle doküman ile uygulama arasında ortaya çıkabilecek farklılıklar durumunda revizyon süreci başlatılmaktadır.

Bilgi Güvenliği sorumluları, yılda en az bir kez uyguladıkları dokümanları gözden geçirerek revizyon gerekip gerekmediği hususunu değerlendirip, revizyon gerektiren dokümanlar için revizyon süreci başlatılmaktadır.

Üniversite Yönetim Sistemlerini etkileyebilecek büyük değişiklikler olması durumunda (örneğin, standardın revize edilmesi, kurum yapısı ile ilgili büyük değişiklikler vb.) Yönetim Temsilcisi ilgili tüm dokümantasyonun gözden geçirilmesini ve gerekli ise revizyon sürecinin başlatılmasını sağlamaktadır.

Revize veya iptal edilen dokümanların web sitesi üzerinden yayınlanan elektronik ortamdaki kopyaları Kalite ve Stratejik Planlama Dairesi tarafından web sitesi üzerinden kaldırılarak personelin

güncelliğini yitirmiş olan dokümana erişimi engellenmektedir. Güncelliğini yitirmiş olan bu dokümanlar Kalite ve Stratejik Planlama Dairesi server üzerinde arşivlenmektedir.

Referans:

KSP.PR.001 Kayıtların Kontrolü Prosedürü
KSP.PR.002 Dokümantasyon Prosedürü
Bİ.PR.001 Bilgi Güvenliği Politikaları Prosedürü
Bİ.PR.002 Bilgi Güvenliği Organizasyon Prosedürü
Bİ.PR.003 İnsan Kaynakları Güvenliği Prosedürü
Bİ.PR.004 Varlık Yönetimi Prosedürü
Bİ.PR.005 Erişim Kontrolü Prosedürü
Bİ.PR.006 Fiziksel Alanlar ve Çevresel Güvenliği Prosedürü
Bİ.PR.007 İşletim Güvenliği Prosedürü
Bİ.PR.008 Haberleşme Güvenliği Prosedürüne
Bİ.PR.009 Sistem Temini, Geliştirme ve Bakım Prosedürü
Bİ.PR.010 Tedarikçi İlişkileri Prosedürü
Bİ.PR.011 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü
Bİ.PR.012 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları Pros.
Bİ.PR.013 BGYS Uyum Prosedürü
Bİ.PR.014 BGYS Risk Analizi Prosedürü

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

EPY.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 **Bİ.PR.014 BGYS Risk Analiz Prosedürü'** ne uygun oluşturulmaktadır.

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.PR.001 Kayıtların Kontrolü Prosedürüne** uygun olarak muhafaza etmektedir.

8.3. Bilgi Güvenliği Risk İşleme

Çalışmalar **Bİ.PR.014 BGYS Risk Analiz Prosedürü'** nde tanımlanmıştır. Bilgi güvenliği risk işlemesinin sonuçlarına ait yazılı bilgileri **KSP.PR.001 Kayıtların Kontrolü Prosedürüne** uygun olarak muhafaza etmektedir.

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.

Kapadokya Üniversitesi izleme ve gözden geçirme prosedürlerini ve diğer kontrolleri gerçekleştirmektedir. Bu kontrolleri gerçekleştirirken;

- Yönetimin, kişilere devredilen ya da bilgi teknolojisince gerçekleştirilen güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığını belirleyebilmesini sağlama,
- Güvenlik olaylarını saptama ve belirteçler kullanarak güvenlik ihlal olaylarını önlemeye yardım etme,
- Bir güvenlik kırılmasını çözmek için alınan önlemlerin etkili olup olmadığına karar verme.

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

Güvenlik denetimlerinin sonuçları, ihlal olayları, etkinlik ölçümleri sonuçları ve tüm ilgili taraflardan önerileri ve geri bildirimleri dikkate alarak BGYS'nin (BGYS politikası ve amaçlarını karşılama ve güvenlik kontrollerini gözden geçirme dahil) etkinliğinin düzenli olarak gözden geçirilmesini üstlenir.

Güvenlik gereksinimlerinin karşılandığını doğrulamak için kontrollerin etkinliğini ölçer.

Aşağıdakilerde oluşacak değişiklikleri dikkate alarak, risk değerlendirmeyi planlanmış aralıklarda ve artık riskleri ve belirlenmiş kabul edilebilir risk seviyelerini gözden geçirir

- Teknoloji,
- İş amaçları ve prosesleri,
- Tanımlanmış tehditler,

- Gerçekleştirilen kontrollerin etkinliği ve
- Yasal ve düzenleyici ortamdaki değişiklikler, değiştirilmiş anlaşma yükümlülükleri ve sosyal iklimdeki değişiklikler gibi dış olaylar.

Planlanan aralıklarda iç BGYS denetimlerini gerçekleştirir.

Kapsamın uygun kalması ve BGYS prosesindeki iyileştirmelerin tanımlanmasını sağlamak için, BGYS' nin yönetim tarafından düzenli olarak gözden geçirilmesini sağlar.

İzleme ve gözden geçirme faaliyetlerindeki bulguları dikkate alarak güvenlik planlarını güncelleştirmesini sağlar.

BGYS etkinliğinde ya da performansında bir etkisi olabilecek eylemleri ve olayları kayıt altına alır.

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.

Denetleme ve değerlendirme faaliyetleri **KYS.PR.003 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.

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 **KSP.PR.007 Yönetimin Gözden Geçirmesi Prosedürü'** ne uygun olarak gözden geçirmektedir. 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.012 YGG Raporu** ile kayıt altına almaktadır. Yazılı bilgiler **KSP.PR.001 Kayıtların Kontrolü Prosedürüne** uygun olarak muhafaza etmektedir. Yönetim Gözden Geçirmesi süreçlerine ilişkin esaslar **YNG.010 Kalite Komisyonu Yönergesinde** tanımlanmıştır.

10. İYİLEŞTİRME

Üniversitemiz Bilgi Güvenliğini en iyi seviyeye ulaştırmak, hizmet düzeyini iyileştirmek-geliştirmek, olası istenmeyen durumları ve uygunsuzlukları önceden tespit etmek, önlemek ve Bilgi Güvenliği performansını artırabilmek amacı ile iyileştirme çalışmaları yapmaktadır. Çalışmalar YGG kararlarının uygulanması, Bilgi Güvenliği toplantıları, veri analizi sonucu elde edilen sonuçların

değerlendirilmesi, SWOT analizi ve düzeltici faaliyet sonuçlarının devreye alınmasıyla gerçekleştirilmektedir.

10.1. Uygunsuzluk ve Düzeltici Faaliyet

Üniversitemiz, talep-şikâyet kutusundaki veriler, çağrı merkezi ve paydaşlarından gelen talep ve şikâyetler, yapılan memnuniyet anketleri ve çözüm destek sistemi verileri dikkate alınarak istenmeyen durumlar belirlenmekte ve iyileştirme faaliyetleri oluşturulmaktadır.
Bu duruma ek olarak analiz edilen verilerin bazı zamanlarda yeni faaliyetleri ve yeni projeleri tetikleyebilmektedir. Bu veriler sayesinde farklı bakış açısı kazanılarak yeni projelerin temeli oluşturulmaktadır. Yapılan projeler, faaliyetler ve yenilikler kayıt altına alınmaktadır.

Kapadokya Üniversitesi, uygunsuzlukların nedenini gidermek ve tekrarını önlemek için gerekli tedbirleri **KSP.PR.005 Düzeltici İşlem Prosedürü'** ne göre almaktadır.

Karşılaşılan uygunsuzluğun sebebini ortadan kaldıracak "düzeltici faaliyet" belirlenir ve uygulanır. Bilgi Güvenliğine yönelik ihlal olaylarında **Bİ.PR.011 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü'** ne göre hareket edilir. 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.PR.005 Düzeltici İşlem Prosedürü

Bİ.PR.011 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, yapılan analiz ve değerlendirmelerin sonuçları ile YGG çıktıları dikkate alınarak sürekli iyileştirme çalışmaları gerçekleştirilir.