BURSA ULUDAĞ ÜNİVERSİTESİ

BGYS EL KİTABI

İçindekiler

1. KAPSAM 3
1.1 Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı Tarihçesi ve Bugünü 3
1.2 Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı Organizasyon Şeması 3
1.3 Misyon, Vizyon ve Değerler 3
1.4 İletişim 3
2. ATIF YAPILAN STANDARD VE/VEYA DOKÜMANLAR 4
3. TERİMLER VE TARİFLER 4
4. KURULUŞUN BAĞLAMI 4
4.1 Kuruluş ve Bağlamının Anlaşılması 4
4.2 İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması 5
4.3 Bilgi Güvenliği Yönetim Sistemi Kapsamının Belirlenmesi 6
4.3.1 Kuruluşun ve Bağlamın Anlaşılması 7
4.4 Bilgi Güvenliği Yönetim Sistemi ve Süreçleri 7
4.4.1 Genel 7
4.4.2 Dokümante Edilmiş Bilginin Sürekliliği ve Muhafazası 8
5. LİDERLİK 8
5.1 Liderlik ve Taahhüt 8
5.1.1 Genel 8
5.2 Politika 8
5.2.1 Bilgi Güvenliği Politikasının Oluşturulması ve Duyurulması 8
5.2.2 Bilgi Güvenliği Politikasının Duyurulması 8
5.3 Kurumsal Görev, Yetki ve Sorumluluklar 9
6. PLANLAMA 9
6.1 Risk ve Fırsatları Belirleme Faaliyetleri 9
6.1.1 Genel 9
6.1.2 Risk Değerlendirme Faaliyetleri 9
6.1.3 Risk İşleme Faaliyetleri 10
6.2 Bilgi Güvenliği Hedefleri ve Planlanması 11
7. DESTEK 11
7.1 Kaynaklar 11
7.1.1 Genel 11
7.1.2 Yeterlilik 11
7.3 Farkındalık 12
7.4 İletişim 12
7.5 Dokümante Edilmiş Bilgi 12
7.5.1 Genel 12
7.5.2 Oluşturma ve Güncelleme 12
7.5.3 Dokümante Edilmiş Bilginin Kontrolü 12
8. OPERASYON 13
8.1 Operasyonel Planlama ve Kontrol 13
8.2 Bilgi Güvenliği Risk İşleme 13
9. PERFORMANS DEĞERLENDİRME 13
9.1 İzleme, Ölçme, Analiz ve Değerlendirme 13
9.1.1 Genel 13
9.2 İç Tetkik 13
9.2.1 Planlama 13
9.2.2 Gereklilikler 14
9.3 Yönetimin Gözden Geçirmesi 14
9.3.1 Genel 14
9.3.2 Yönetimin Gözden Geçirmesi Girdileri 14
9.3.3 Yönetimin Gözden Geçirmesi Çıktıları 14
10. İYİLEŞTİRME 14
10.1 Genel 14
10.2 Uygunsuzluk Yönetimi, Düzeltici ve İyileştirici Faaliyet 15
10.3 Sürekli İyileştirme 15
İLGİLİ DOKÜMANLAR 15
SON HÜKÜMLER 15
EKLER 15

ÖNSÖZ

Bilgi güvenliği yönetim sistemi (BGYS), Bursa Uludağ Üniversitesi bünyesindeki her türlü bilgi işlem teknolojilerini yürütülmekle esas görevli olan Bilgi İşlem Daire Başkanlığı'nda bilgi güvenliğinin sağlanması için; programları, politikaları ve amaçları ortaya koyar.

Bilgi İşlem Daire Başkanlığında verilen hizmetlerde "Bilgi Güvenliği" ana hareket noktalarından bir tanesi olarak belirlenmiştir. Başkanlığı'mızdan hizmet alan kişi, kurum ve kuruluşlara, dürüst ve prensipli kararlarla Bilgi Güvenliği standartlarına uygun hizmet vermeyi kendisine amaç edinmiştir.

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

Bursa Uludağ Üniversitesi misyonu ve vizyonu çerçevesinde vermiş olduğumuz hizmetlerde Bilgi Güvenliğini ana önceliklerden bir tanesi olarak belirlemiş durumdayız.

1. KAPSAM

1.1 Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı Tarihçesi ve Bugünü

11 Nisan 1975 tarih ve 15205 sayılı Resmi Gazetede yayınlanan 1873 sayılı kanun ile Bursa'da Bursa Üniversitesi olarak kurulan Üniversitemizde Bilgi İşlem Daire Başkanlığı Mart 1983'te faaliyetlerine başlamıştır.

Bilgi İşlem Daire Başkanlığı web sayfasında tanıtım ve tarihçe başlığı altında detaylı bilgi yer almaktadır.

1.2 Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı Organizasyon Şeması

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı organizasyon şeması Bilgi İşlem Daire Başkanlığı web sayfasında yer almaktadır.

1.3 Misyon, Vizyon ve Değerler

Bilgi İşlem Daire Başkanlığımız misyon, vizyon değerleri ile Üniversitemiz temel değerleri benimsenmektedir.

MİSYON: Misyonumuz; dünyanın saygın üniversitelerinin bilgi işlem birimleri ile kıyaslanabilir kalite ve teknolojiye sahip olabilmektir.

VİZYON: Türkiye'deki üniversiteler arasında bilişim altyapısı, kullanıcı memnuniyeti, düzenlenen etkinlikler, verilen hizmet kalitesi ve çeşitliliği bakımından en üst sıralara yerleşmek; Teknolojiyi yakından izleyerek, üniversitemizin bilgi işlem sistemini yürütmek, eğitim, öğretim ve araştırmalara destek sağlamak, Üniversitemizin ihtiyaç duyacağı diğer bilgi işlem hizmetlerini eksiksiz olarak yerine getirmektir.

TEMEL DEĞERLER:

Ortak Akıl ve Katılımcılık

Etik Değerlere Bağlılık

Kurumsal Aidiyet

Yenilikçilik ve Girişimcilik

Çevreye Saygı ve Duyarlılık

Evrensel ve Toplumsal Değerlere Saygı

Yerel ve Toplumsal Kalkınmaya Destek

1.4 İletişim

Ünvanı: Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı

Adresi: Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı (Yeni Bina) Görükle Kampusu PK:16059 Görükle/BURSA

Web Adresi: https://uludag.edu.tr/bilgiislem

Mail Adresi : **bidb@uludag.edu.tr**

2. ATIF YAPILAN STANDARD VE/VEYA DOKÜMANLAR

- TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (Sistemimiz içerisinde ilgili standart dokümanlarda yer alırken, versiyonu yazılmayacak olup bu maddede son versiyon tanımlanmıştır).
- Üniversitemiz Yönetim Sistemleri Kapsamında oluşturulan tüm iç ve dış kaynaklı dokümanlar.

3. TERİMLER VE TARİFLER

Bilgi güvenliği yönetim sisteminin standarda uygunluğu açısından, TS EN ISO/IEC 27001 BGYS standardında verilen terimler ve tarifler uygulanır.

Bilgi Varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir.

İş Süreçleri **:** İşin yapılması ile ilgili tüm adımların belirlendiği süreçlerdir.

Gizlilik **:** Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır.

Bütünlük **:** Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır.

Erişilebilirlik (Kullanılabilirlik): Bir varlığın yetkili varlıklarca talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Risk **:** Bir tehdidin olasılığı ile şiddetinin bileşkesi şeklinde ele alınır. Bir varlığın zarara, kayba uğrama tehlikesidir.

Paydaş: Hizmetlerimizden dolaylı olarak etkilenen ilgili diğer taraflardır: Sivil Toplum Kuruluşları, İşletmeler, ilişkide bulunulan diğer Kamu Kuruluşları, Üniversiteler…

4. KURULUŞUN BAĞLAMI

4.1 Kuruluş ve Bağlamının Anlaşılması

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı, sağlamış olduğu hizmetlerde, yasal ve mevzuat şartlarının gerektirdiği düzeyde Bilgi Güvenliği faaliyetlerini yürütmeyi hedeflemektedir. Bilgi güvenliği risklerini tanımlamak ve riskleri bertaraf etmek hedeflenmektedir.

Üniversitemiz Stratejik amaçlarına uygun olarak; Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Politikası doğrultusunda Bilgi Güvenliği Yönetim Sistemimiz ile ilgili hedeflere ulaşılmasında etkisi olacak iç ve dış hususlar aşağıdaki gibi tayin edilmiştir.

İç hususlar;

- Başkanlığımızın iç organizasyonu; tanımlanan roller ve yükümlülükler,
- Yerine getirilecek politikalar, hedefler ve stratejiler,

- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (zaman, kişiler, süreçler, sistemler, teknolojiler, vs.),
- Kurum kültürü,
- Bilişim sistemleri, bilgi akışı, karar alma süreçleri,
- Kurum tarafından uyarlanan standartlar, kılavuzlar, modeller,
- Fiziksel alt yapı yeterliliği,
- İç paydaşlarla ilişkiler, onların algılamaları ve değerleri,

Dış hususlar;

- YÖK tarafından belirlenen kurallar,
- Eğitim Hizmetleri ve Araştırma-Geliştirme faaliyetleri için yayınlanan yasal şartlar (Kanun, Yönetmelik, Talimat, Genelge, Tebliğ vb.)
- Kuruluşun hedefleri üzerinde etkisi bulunan yönetim ve denetim mekanizmaları,
- Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri,

Olarak belirlenmiştir.

Belirlenen iç ve dış hususlarla ilgili bilgi izlenmekte ve Yönetimi Gözden Geçirme toplantılarında değerlendirilmektedir. ***BUÜ Stratejik Planı (Güncel Versiyonu)***

PL 001_İlgili Taraf Beklenti v e İstek Planı

4.2 İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

a) Bilgi Güvenliği Yönetim Sistemi ile İlgili Taraflar

Bilgi Güvenliği Yönetim Sistemi ile ilgili taraflar:

1) Bursa Uludağ Üniversitesi Tüzel Kişiliğini temsil eden Üst Yönetim,

2) Personel,

3) Tedarikçiler,

4) Öğrenciler,

5) Misafirler öğrenciler,

6) Misafir öğretim elemanları,

7) Dış Paydaşlar

b) Tarafların Bilgi Güvenliği İle İlgili Gereksinimleri:

Bilgi Güvenliği Yönetim Sistemi ile ilgili beklentileri:

İlgili Taraf	Beklentiler
Bursa Uludağ Üniversitesi Tüzel Kişiliğini temsil eden Üst Yönetim	- Kurum prestijinin korunması, - Kurumun elde ettiği bilgi birikiminin korunması, - Yasal şartlara uyum,
Personel	- Yasal şartlara uyum, - BT sistemlerinde sunulan hizmetlerin kesintisiz sağlanması,
Tedarikçiler	- Yasal mevzuatın eksiksiz uygulanması, - Süreklilik, - Karşılıklı güven,
Öğrenciler	- Yasal şartlara uyum, - BT sistemlerinde sunulan hizmetlerin kesintisiz sağlanması,
Misafirler öğrenciler	- Yasal şartlara uyum, - BT sistemlerinde sunulan hizmetlerin kesintisiz sağlanması.
Misafirler öğretim elemanları	- Yasal şartlara uyum, - BT sistemlerinde sunulan hizmetlerin kesintisiz sağlanması.
Dış Paydaşlar	- Yasal şartlara uyum - Geri bildirim sistemi - İstek ve şikâyetlerin dikkate alınması

4.3 Bilgi Güvenliği Yönetim Sistemi Kapsamının Belirlenmesi

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı'nın mevcut faaliyet alanları için, tarafların şartlarını karşılamak amacıyla TS EN ISO/IEC 27001 standardına uygun olarak bir Bilgi Güvenliği Yönetim Sistemi kurulmuştur. Kurulan sistem Bilgi İşlem Daire Başkanlığına ait tüm bölümlerini, çalışanları, dış hizmet aldığımız tedarikçilerimiz, hizmet verdiğimiz öğrenciler ve üniversitemize gelen misafirlerimizi/ziyaretçilerimiz için uygulanmaktadır.

Bilgi Güvenliği Yönetim Sistemimizin kapsamı Bilgi İşlem Daire Başkanlığı hizmetlerindeki kayıtların bilgi varlıklarının korunmasıdır.

Bursa Uludağ Üniversitesi olarak TS EN ISO/IEC 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

Kapsam: Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından yerine getirilen tüm faaliyetler.

Lokasyon: Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı (Yeni Bina) Görükle Kampusu PK:16059 - **Görükle/BURSA**

Hariç Maddeler: Kapsam dışı bırakılan Ek-A kontrol maddesi bulunmamaktadır.

4.3.1 Kuruluşun ve Bağlamın Anlaşılması

Dış Bağlam

Dışarıdan aldığımız hizmetler; Destek Hizmetleri, Danışmanlık hizmetleri, İnternet servis sağlayıcı hizmetleridir. Üniversitemizin diğer birimleri, tedarikçilerimiz ve ilgili diğer 3. taraflarla ilişkileri kapsar.

İç Bağlam

Bilgi Güvenliği Yönetim sistemi aşağıdaki faaliyetleri ve bu faaliyetlerin yürütüldüğü bina ve ofisleri kapsar.

- İdari ve Mali Hizmetler Birimi
- Yazılım ve Veritabanı Yönetimi Birimi
- Sunucu Sistemler Yönetim Birimi
- Bilgi ve İletişim Güvenliği (Siber Güvenlik) Birimi
- Ağ Yönetim Birimi
- Web Tasarım ve Yönetim Birimi
- Kullanıcı Destek Hizmetleri Birimi

Yukarıda tanımlanan süreçler ve bu süreçlere ait bilgi varlıkları hazırlanan varlık envanterinde tanımlanmıştır. BGYS içerisinde kullandığımız teknolojiler; Sunucular, bilgisayarlar, donanımlar, yazılımlar, Güvenlik Sistemleri ve Haberleşme cihazlarıdır.

BGYS aşağıdakilerin hepsini kapsar ;
- Üniversitemize emanet edilen bilgileri
- Üniversite çalışanları ve öğrencilerimize ait kişisel bilgiler
- Üniversitemizin tüm kurumsal ve kişiye özel bilgileri
- Yukarıdaki bilgileri içeren BT (Bilgi Teknolojileri) Sistemleri
- Tedarikçi sözleşmeleri.
- Dış kaynak kullanım sözleşmeleri.
- Hizmet sunulan ofis, oda, binalarda bulunan tüm araç ve gereçler.
- Sistem Dokümantasyonu

4.4 Bilgi Güvenliği Yönetim Sistemi ve Süreçleri

4.4.1 Genel

Üniversitemizde, TS EN ISO/IEC 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.

LS 001- Bursa Uludağ Üniversitesi Süreç Listesi

4.4.2 Dokümante Edilmiş Bilginin Sürekliliği ve Muhafazası

Süreçler ve bu süreçlerin yönetilmesi için gerekli olan tüm dokümante edilmiş bilgiler web sayfasından erişilebilen uygulama üzerinden ulaşılabilir durumdadır.

www.unikys.uludag.edu.tr

5. LİDERLİK

5.1 Liderlik ve Taahhüt

5.1.1 Genel

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 ve Duyurulması

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Politikası üst yönetim tarafından Kurumun amaç ve bağlamına uygun, misyon ve vizyona kaynak sağlayacak prensipte belirlenmiş, onaylanmış ve yürürlüğe alınmıştır. Bilgi Güvenliği politikası uygulanabilir şartların yerine getirilmesi ve sürekli iyileştirme için taahhüt içermektedir.

Bilgi Güvenliği Politikası

5.2.2 Bilgi Güvenliği Politikasının Duyurulması

Bilgi Güvenliği Politikasının Kurumdaki personel ve tüm paydaşlar tarafından bilinirlik ve anlaşılırlığını sağlamak için "Bilgi Güvenliği El Kitabı" hazırlanmış ve verilen eğitimlerle anlaşılması sağlanmıştır. Ayrıca ***https://uludag.edu.tr/bilgiislem*** web sitesinde yayınlanarak ilgili tarafların erişimine açılmıştır.

YD 005 BGYS El Kitabı

5.3 Kurumsal Görev, Yetki ve Sorumluluklar

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yürütülen süreçlerin etkinliğinin ve amaçlanan sonuçlara ulaşmasının sağlanması için Bilgi Güvenliği Yönetim Sistemi ile ilgili roller belirlenmiştir. Bilgi Güvenliği Yönetim Sistemi kapsamında yürütülecek çalışmaların planlanması ve takibi Kalite Koordinatörlüğü tarafından organize edilecek ve yönetilecektir.

Kurumsal görev, yetki ve sorumluluklar ilgili mevzuat ile belirlenmiş olup, verilen görev ve sorumlulukları da içeren görev tanımları hazırlanmıştır. Görev tanımları ve Organizasyon şeması iç kontrol sistemi sayfası ile tüm çalışanlara duyurulmuştur. Görevlerin gerektirdiği nitelikler yine görev tanımları içinde yer almaktadır.

Organizasyon Şeması Bilgi İşlem Daire Başkanlığı WEB Sitesinde yayınlanmaktadır.

Görev Tanımları (İç Kontrol Otomasyonunda bulunmaktadır)

6. PLANLAMA

6.1 Risk ve Fırsatları Belirleme Faaliyetleri

6.1.1 Genel

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı, 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 Bursa Uludağ Üniversitesi tarafından oluşturulan Kurumsal Risk Yönetimi Strateji Belgesi uygulanmaktadır. **(BUÜ Strateji Geliştirme Daire Başkanlığı Web sayfasında yayındadır.)**

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

b) İstenmeyen etkileri önlemek veya azaltmak,

c) Sürekli iyileşmenin başarılması,

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı 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.

6.1.2 Risk Değerlendirme Faaliyetleri

Üniversitemiz, akademik ve idari birimlerinde Bilgi Güvenliğini sağlamak ve geliştirmek için Kurumsal Risk Yönetimi Strateji Belgesi 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 Kurumsal Risk Yönetimi Strateji Belgesine göre 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,

Bilgi İşlem Daire Başkanlığı bilgi güvenliği risk değerlendirme süreci ile ilgili olarak yazılı bilgilerin muhafaza edileceği yapıyı kurmuş ve işletmektedir.

FR 3.3.2_18 BGYS Risk İşleme Plan Formu

6.1.3 Risk İşleme Faaliyetleri

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı 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,

6.2 Bilgi Güvenliği Hedefleri ve Planlanması

Bilgi İşlem Daire Başkanlığı ilgili fonksiyon ve seviyelerinde Bilgi Güvenliği amaçlarının takip edilebilmesi ve değerlendirilmesi amacıyla FR 3.3.2_12 BGYS Hedef ve Performans Değerlendirme tablosu oluşturulmuştur. 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.

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.

FR 3.3.2_17 BGYS Hedef ve Performans Değerlendirme Tablosu

7. DESTEK

7.1 Kaynaklar

7.1.1 Genel

Bilgi Güvenliği Yönetim Sisteminin uygulanmasına, sürdürülmesine, sürekli iyileştirilmesine, tüm paydaşların ihtiyaç ve beklentilerinin yerine getirilmesi için gerekli kaynak ihtiyacı belirlenmekte ve karşılanmaktadır. Temel ve Alt Süreç sorumluları kaynak ihtiyaçlarını tespit etmekten sorumludur. İhtiyaç duyulan kaynaklar ilgili mevzuat ve bütçe kapsamında belirlenmekte ve tedarik edilmektedir.

7.1.2 Yeterlilik

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı 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.

Üst Yönetim çalışanların eğitim ve yetkinlik ihtiyaçlarını karşılamak üzere gerekli tedbirleri alarak eğitim ihtiyaç analizi ile çalışanların eğitim almalarını sağlamaktadır.

7.3 Farkındalık

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından, tüm çalışanlarının; bilgi güvenliği politikası, ilgili bilgi güvenliği hedefleri, BGYS "nin etkinliğine yapılan katkılar, Bilgi Güvenliği Yönetim Sistemi şartlarının yerine getirilmemesi durumunda oluşabilecek sonuçların farkındalığı için hizmet içi eğitimler düzenlenmektedir.

Çalışanların eğitim ve yetkinlik ihtiyaçlarını karşılamak üzere gerekli tedbirleri alarak eğitim ihtiyaç analizi ile çalışanların eğitim almalarını sağlamaktadır.

FR 3.1.2_02 Yıllık Eğitim Planı

PR 005 Hizmet İçi Eğitim Prosedürü

7.4 İletişim

Üst yönetim hizmetler ve Bilgi Güvenliği Yönetim Sisteminin yürütülmesi için gerekli olan iç ve dış iletişimi eksiksiz olarak sağlayabilmek için, zaman zaman dikey, işin niteliğine göre zaman zaman da farklı fonksiyon ve seviyeler arasında yatay olarak yerine getirilmesini temin edebilmek amacıyla farklı iletişim yöntemleri kullanmaktadır. BUÜ"de bu tür faaliyetler "*PL 002_BUÜ İletişim Rehberi Planı'*nda belirtilen usullerde yapılmaktadır.

PL 002_BUÜ İletişim Rehberi Planı

7.5 Dokümante Edilmiş Bilgi

Üniversitenin gerçekleştirdiği faaliyetlerin genel çerçeveleri; faaliyetler gerçekleştikten sonra elde edilen verilerin işlenmesine, muhafaza edilmesine ve elden çıkarılmasına yönelik yapılan tüm işlemler dokümante edilmiş bilgi yönetimi olarak değerlendirilmektedir.

7.5.1 Genel

Üniversite BGYS süreçlerinin etkili ve verimli bir şekilde yürütülmesini sağlamak amacıyla BGYS dokümanları hazırlanmakta ve gözden geçirilerek iyileştirilmektedir. BGYS dokümanlarına "https://uludag.edu.tr/kalite" web adresinden ulaşılabilmektedir.

7.5.2 Oluşturma ve Güncelleme

7.5.1'de ifade edilen Üniversite KYS ve Bilgi Güvenliği dokümantasyonunun oluşturulması ve güncellenmesi faaliyetleri "*PR 001_Dokümante Edilmiş Bilginin Yönetimi Prosedürü* "ne uygun olarak sürdürülmektedir.

PR 001_Dokümante Edilmiş Bilginin Yönetimi Prosedürü

7.5.3 Dokümante Edilmiş Bilginin Kontrolü

Dokümante Edilmiş Bilginin Kontrolü 7.5.1'de ifade edilen "*PR 001_Dokümante Edilmiş Bilginin Yönetimi Prosedürü*" ne uygun olarak sürdürülmektedir.

8. OPERASYON

8.1 Operasyonel Planlama ve Kontrol

Bilgi güvenliği şartlarını karşılamak ve Madde 6.1'de belirlenen faaliyetleri gerçekleştirmek için gerekli olan süreçler planlanmış, uygulanmakta ve kontrol edilmektedir. Madde 6.2'de belirlenen bilgi güvenliği amaçlarını başarmak için aynı zamanda planlar uygulanır. Süreçlerin planlandığı gibi yürütüldüğünden emin olunan noktaya kadar yazılı bilgiler saklanır. Planlanan değişiklikler kontrol edilir ve istenmeyen değişikliklerin sonuçları gözden geçirilerek, gerekiyor ise kötü etkileri azaltmak için eyleme geçilir.
Bilgi İşlem Daire Başkanlığı süreçleri BUÜ Kalite Koordinatörlüğü web sayfasında Üniversite Kalite Yönetim Sayfasında yer almaktadır.

8.2 Bilgi Güvenliği Risk İşleme

Madde 6.1.2 a) da belirtilen kriterler dikkate alınarak, bilgi güvenliği risk değerlendirmeleri yılda en az bir kez gözden geçirilir. Önemli değişiklikler önerildiğinde veya meydana geldiğinde bu gözden geçirme süresi beklenmez.
FR 3.3.2_18 BGYS - Risk İşleme Plan

9. PERFORMANS DEĞERLENDİRME

9.1 İzleme, Ölçme, Analiz ve Değerlendirme

9.1.1 Genel

Bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliği değerlendirilir.

a) Bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere neyin izlenmesi ve ölçülmesinin gerekli olduğu,
b) Geçerli sonuçları temin etmek için, uygun İzleme, ölçme, analiz ve değerlendirme yöntemleri,
c) İzleme ve ölçmenin ne zaman yapılacağı,
d) İzlemeyi ve ölçmeyi kimin yapacağı,
e) İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği ve
f) Bu sonuçları kimin analiz edeceği ve değerlendireceği.

Belirlenmiştir.
Performans değerlendirme sonuçları FR 3.3.2_12 BGYS Hedef ve Performans Değerlendirme tablosu üzerinden takip edilmekte ve YGG toplantıları aracılığıyla üst yönetime sunulmaktadır.

9.2 İç Tetkik

9.2.1 Planlama

İç tetkik planı her akademik yıl başlangıcında Kalite Koordinatörlüğü tarafından PR 004 İç Tetkik Prosedüründe tanımlandığı gibi "PL 003_İç Tetkik Planı" hazırlanır. BGYS İç Tetkik Planı, tüm birimlerin her akademik dönem içerisinde en az bir defa denetlenmesini sağlayacak şekilde hazırlanır. Bununla birlikte tetkik sıklığı belirlenirken, Kalite Koordinatörlüğü tarafından önceki tetkik sonuçları ve denetlenecek birimin önem ve durumu dikkate alınır. İhtiyaç duyulan birimlerin daha sık denetlenmesi sağlanabilir.

PL 003_ İç Tetkik Planı

PR 004_ İç Tetkik Prosedürü

9.2.2 Gereklilikler

Üniversitemizde, Bilgi Güvenliği Yönetim Sisteminin ilgili BGYS standardı ve yasal mevzuat şartlarını karşıladığını ve etkin olarak sürdürüldüğünü doğrulamak için planlı iç tetkik faaliyetleri yürütülmektedir.

PR 004_ İç Tetkik Prosedürü

PL 003_ İç Tetkik Planı

9.3 Yönetimin Gözden Geçirmesi

9.3.1 Genel

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı olarak yılda bir kez Yönetimi Gözden Geçirme Toplantısı BGYS kapsamı dahilinde yapılarak Üniversitemizin Üst Yönetimine raporlanır.

PR 002_Yönetim Gözden Geçirme Prosedürü

9.3.2 Yönetimin Gözden Geçirmesi Girdileri

- Süreç performansları
- Sürekli iyileştirme Formları
- Bir önceki YGG takip faaliyeti
- Bilgi Güvenliği Hedefleri
- Bilgi Güvenliği Politikası
- Erişim Kontrolü Politikası
- İlgili Taraflardan gelen bildirimler
- Olay Kayıtları
- Risk İşleme Planı vb.
- İç ve dış tetkik sonuçları

9.3.3 Yönetimin Gözden Geçirmesi Çıktıları

Gözden geçirme çıktısı, Bilgi Güvenliği Yönetim Sisteminin ve süreçlerin etkinliğinin değerlendirilmesi, müşteri şartları ile ilgili hizmetin iyileştirilmesi ve ihtiyaçların saptanmasıdır. Karar ve faaliyetler toplantı Tutanak Katılım Tutanak Formuna kayıt edilerek toplantı üyelerine dağıtılır.

PR002_Yönetim Gözden Geçirme Prosedürü

10. İYİLEŞTİRME

10.1 Genel

Üniversitemiz hizmet kalitesini en iyi seviyeye ulaştırmak, hizmet düzeyini iyileştirmek- geliştirmek, olası istenmeyen durumları ve uygunsuzlukları önceden tespit etmek, önlemek ve hizmet kalitesi performansını artırabilmek amacı ile iyileştirme çalışmaları yapmaktadır. Bu çalışmalar "PR 003_Sürekli İyileştirme Prosedürü" doğrultusunda gerçekleştirilir. YGG kararlarının uygulanması, kalite toplantıları, veri analizi

sonucu elde edilen sonuçların değerlendirilmesi, SWOT analizi ve düzeltici faaliyet sonuçlarının devreye alınmasıyla sürekli iyileştirme faaliyetleri gerçekleştirilir.

PR 003_Sürekli İyileştirme Prosedürü

10.2 Uygunsuzluk Yönetimi, Düzeltici ve İyileştirici Faaliyet

Üniversitemiz, talep-şikâyet kutusundaki veriler, öneri 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.

10.3 Sürekli İyileştirme

Üniversitemiz, Bilgi Güvenliği Yönetim Sistemi çerçevesinde sürekli iyileştirme felsefesini benimsemiş ve kabul etmiştir. Bu kapsamda yeni projeler ve faaliyetler gerçekleştirilmekte, bu projelerin ve faaliyetlerin her geçen gün artması için çalışmalar yapılmakta ve bu tür çalışmaların artması sağlanmaktadır. Yapılan analiz ve değerlendirmelerin sonuçları ile YGG çıktıları dikkate alınarak sürekli iyileştirme çalışmaları gerçekleştirilir.

PR 003_Sürekli İyileştirme Prosedürü

İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği Yönetim Sistemi Kapsamında hazırlanan, yararlanılan tüm bilgi ve belgeler.
- TS EN ISO/IEC 27001 BGYS Standardı
- Prosedürler
- Formlar
- Listeler
- Organizasyon Şemaları
- Görev Tanımları
- İç Kaynaklı Dokümanlar
- Dış Kaynaklı Dokümanlar vb...

SON HÜKÜMLER

TS EN ISO/IEC 27001 BGYS standardı kapsamında hazırlanan tüm bilgi ve belgeler Bilgi İşlem Daire Başkanlığı liderliğinde hazırlanmış olup, uygulanmasından güncelleştirilmesinden, iyileştirilmesinden Bursa Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı tüm personeli sorumludur.

EKLER