

T.C.

KONYA TEKNİK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönerge; Üniversitemizin ihtiyaç duyduğu bilginin üretilmesi, işlenmesi, saklanması ve iletilmesi sürecinde; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan, kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak; ilgili yasalara, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) gereklerine, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesine, 5651 Sayılı Kanunu Gereklerine, TÜBİTAK ULAKBİM’in ilgili politikalarına ve TS ISO/IEC ISO 27001 Bilgi Güvenliği Yönetim Sistemi standartlarına uygun olarak yürütülen faaliyetlerin adil, etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini sağlayacak kuralları belirlemek ve ilgili politikaları üretmek amacıyla hazırlanmıştır.

Kapsam

MADDE 2 - (1) Bu Yönerge; Konya Teknik Üniversitesi personeli ve öğrencileri ile kendilerine herhangi bir nedenle geçici veya kalıcı veya kısıtlı olarak Konya Teknik Üniversitesi Bilişim Kaynaklarını kullanma, yönetme veya izleme olanağı sunulan kişileri, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini, hizmet sağlayıcılarını, sistem, veri ve bilgi kullanıcılarını ve kurallarını kapsar.

Dayanak

MADDE 3 - (1) Bu Yönerge, 5237 sayılı Türk Ceza Kanunu’nun İkinci Kısmı (Kişilere Karşı Suçlar) Dokuzuncu Bölümü (Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar-132, 133, 134, 135, 136, 137, 138, 139, 140. Maddeler), Üçüncü Kısmı (Topluma Karşı Suçlar) Onuncu Bölümü (Bilişim Alanında Suçlar-243, 244, 245, 246. Maddeler), 5070 sayılı “Elektronik İmza Kanunu”, 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”, 2547 sayılı Yükseköğretim Kanununun 12. Maddesi ile 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, 2007/4 Sayılı “Kamu Kurumları İnternet Sitesi Kılavuzu” Genelgesine, 6698 Sayılı Kişisel Verilerin Korunması Kanunu’na, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesine, Ulusal Akademik Ağ (ULAKNET) Kullanım Politikasına ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standartlarına ve diğer ilgili mevzuat hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu yönergede geçen;

1. Bilgisayar Ağı: Elektronik cihazlar arasında veri/bilgi aktarımı ve etkileşimini sağlayan, geniş ve dar alanlar bütünlüğünde fiziki ağ yapısı ile bunu destekleyen ve kullanımını gerçekleştirmeye yarayan tüm donanım ve yazılımların oluşturduğu sistemi,
2. Bilgi Güvenliği Yönetim Sistemleri (BGYS): ISO 27001 Bilgi güvenliği kalite standartları ve bu standartların yönetimini,
3. Bilgi Güvenliği Yönetim Sistemi Politika ve Prosedürleri: Bir kurumun değerli bilgilerinin yönetimini, dağıtımını ve korunmasını düzenleyen kurallar ve uygulamalar bütünü olup, bu politika ve prosedürler, genel Bilgi Güvenliği Politikaları ve belirli

alanlara ait prosedürlerden oluşan ve uygulamaları tanımlayan talimatlarla belirlenen diğer dokümanları,

4. Bilişim Kaynakları: Bilgisayar ağı, kablolu veya kablosuz elektronik cihazlar, aktif veya pasif ağ cihazları, internet altyapısı, taşınabilir bilgi işleme ve depolama cihazları, mobil bilgisayarlar, yazıcı, tablet, telefon, kamera, bilgisayar sistemi, donanımı, yazılımı ve hizmetlerinin tümünü,
5. Bilgi İşlem Daire Başkanlığı (BİDB): Konya Teknik Üniversitesi adına, Konya Teknik Üniversitesi bilişim kaynaklarını yönetme, koordine etme, geliştirme, kontrol etme, her türlü destek işlemleri ile hizmetlerin tümünü gerçekleştiren yetkili birimi,
6. Diğer Kullanıcılar: Konya Teknik Üniversitesi Bilişim Kaynaklarının kullanım hakkına sahip Esas Kullanıcılar dışındaki, özel veya tüzel kişiliğinde olup kullanım hakları ve biçimleri Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından belirlenen tüm kısıtlı veya geçici kullanım hakkı verilmiş kullanıcıları,
7. Esas Kullanıcılar: Konya Teknik Üniversitesi Bilişim Kaynaklarını eğitim-öğretim, araştırma, yönetim ve hizmet faaliyetleri çerçevesinde kullanan Konya Teknik Üniversitesi akademik ve idari görevlerindeki kadrolu, geçici veya sözleşmeli personel ile Konya Teknik Üniversitesinde öğrenimini sürdürmekte olan kayıtlı tüm ön lisans, lisans ve lisansüstü öğrencilerini,
8. İnternet Altyapısı: Ulusal ve uluslararası bilgisayar ağı üzerinde tüm kullanıcı uçlarının adres yapılarını ve veri/bilgi iletişimi kurallarını içeren belirli protokoller ile etkileşimi ve iletişimini sağlayan sistemi,
9. Kişisel Bilişim Kaynakları: Mülkiyeti veya kullanım hakkı Konya Teknik Üniversitesine ait olmayan “Bilişim Kaynakları”nı,
10. Komisyon: Konya Teknik Üniversitesi Bilgi Güvenliği Yönetim Sistemi (BGYS) Komisyonunu,
11. Konya Teknik Üniversitesi Bilişim Kaynakları: Mülkiyeti veya kullanım hakkı Konya Teknik Üniversitesine ait olan “Bilişim Kaynakları”nı,
12. Senato: Konya Teknik Üniversitesi Senatosunu,
13. Üniversite: Konya Teknik Üniversitesini,

İfade eder.

İKİNCİ BÖLÜM

Komisyon Oluşumu ve Görevleri

Komisyon Oluşumu

MADDE 5- (1) Komisyon üyeleri, Üniversite Senatosu tarafından belirlenir.

(2) Komisyon Başkanı, aynı zamanda komisyon üyesi olan Rektör Yardımcısı'dır. Komisyon üyelerinin görev dağılımları, komisyondan üye çıkarılması veya belirlenmesi komisyon başkanının önerisi ile senato tarafından gerçekleştirilir.

(3) Komisyon, Genel Sekreter, Bilgi İşlem Daire Başkanı, Personel Daire Başkanı, Öğrenci İşleri Daire Başkanlığı, akademik birimleri temsil eden üyelerden oluşur. İhtiyaç halinde diğer birimlerden de üye seçimi yapılabilir.

(4) Komisyona, Başkanın önerisi ile senato tarafından üniversite bünyesindeki birimlerden üç yıl için yeni üyeler belirlenebilir. Bu üyeler, gerektiğinde aynı yöntem ile görevden alınabilir.

(5) Komisyon teklifi ile Komisyon Başkanı, alt komisyonlar oluşturabilir.

Komisyon Üyelerinin Görevleri

MADDE 6- (1) Tüm üyeler, komisyon başkanının BGYS düzenlemeleri kapsamında verdiği

görevleri yapmakla ve BGYS uyumuna aktif katkı sağlamakla yükümlüdür. Bununla birlikte üyelerin ek görevleri aşağıdaki şekildedir:

- a) Rektör Yardımcısı: komisyon başkanı olarak komisyonun görevlerinin yerine getirilmesinden, koordinasyonundan, toplanmasından, komisyon kararlarının yürütülmesinin sağlanmasından, yönetim ve iletişiminden sorumludur.
- b) Bilgi İşlem Daire Başkanı: BGYS düzenlemelerine uyum sağlanabilmesi için gerekli olan çalışmaları (politika, prosedür, talimat vb.) yürütür ve komisyona sunar.
- c) BYGS kapsamında komisyona gelen gündem konularını değerlendirir ve gerekli çalışmaları yapar,

ÜÇÜNCÜ BÖLÜM

Komisyonun Görev ve Yetkileri, Usul ve Esasları

Komisyonun Görev ve Yetkileri

MADDE 7- (1) BGYS uyum süreçlerinin işletilmesine ve geliştirilmesine yönelik yöntemler belirler, geliştirir, yöntemlerin uygulanmasını ve denetimini sağlar/sağlatır.

(2) Üniversitenin BGYS gerekliliklerinin yerine getirilmesini sağlar/sağlatır.

(3) Gündeme getirilen konularda alınması gerekli kararları görüşüp karara bağlar.

(4) BGYS ile ilgili konularda, Üniversite Yönetim Kurulunu hem mevcut durum hem de riskler hakkında yılda en az bir kez bilgilendirir.

(5) Komisyon, gerektiğinde Bilgi İşlem Daire Başkanlığının önerilerini de dikkate alarak bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması kapsamında gerekli teknik ve idari tedbirlerin alınmasını sağlamakla yükümlüdür.

Komisyonun Çalışma Usul ve Esasları

MADDE 8- (1) Komisyon olağan olarak altı ayda bir, komisyon başkanının çağrısı veya komisyon üyelerinin salt çoğunluğunun yazılı başvurusuyla toplanır.

(2) Toplantı gündemi, tarihi ve yeri (yüz yüze veya online) Başkan tarafından belirlenir, bu bilgiler Bilgi İşlem Daire Başkanlığı aracılığıyla üyelere duyurulur.

(3) Komisyon, üye tam sayısının salt çoğunluğu ile toplanır ve toplantıya katılanların salt çoğunluğu ile karar alır. Oylarda eşitlik olması halinde, başkanın bulunduğu taraf çoğunluğu sağlamış sayılır.

(4) Komisyonun her toplantısı ve alınan kararlar toplantı tutanağına işlenerek Bilgi İşlem Daire Başkanlığı tarafından dosya veya bilgisayar ortamında arşivlenir.

DÖRDÜNCÜ BÖLÜM

Temel İlkeler

Temel ilkeler

MADDE 9 – (1) Üniversitemizde yer alan bölüm ve birimlerde, başta kişisel veriler olmak üzere, yazılı veya elektronik ortamda saklanan veya sözlü olarak ifade edilen her türlü bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla BGYS tesis edilir.

(2) - BGYS'nin tesis edilmesi ve etkin bir şekilde işletilmesi için, üst yönetim desteği ve katılımı zorunludur.

- (3) - BGYS tesis edilmesi için alınması gereken tedbirler, bilgi güvenliği yönetim sistemi politikaları ve üniversitenin kendisine özgü güvenlik ihtiyaçları dikkate alınmak suretiyle ayrıntılı olarak belirlenir, yazılı hale getirilir ve komisyon geçtikten sonra tüm kullanıcılara duyurulur.
- (4) - Etkin bir BGYS tesis edilmesi için risk yönetimi yapılır. Tespit edilen riskler için riski azaltacak veya kaldıracak tedbirler belirlenir, komisyona sunulur ve uygulanır. Risk yönetimi süreçleri süreklilik arz eder.
- (5) - Bilgi işleme faaliyetlerinin büyük oranda siber ortam üzerinden yapılması nedeniyle, siber güvenlik tedbirlerinin alınması için azami özen gösterilir.
- (6) - Bilgi güvenliğinin sağlanması için sadece siber güvenlik ile ilgili tedbirlerin alınması yeterli değildir. Personel, evrak, ekipman, fiziksel ve çevre güvenliği için de güvenlik tedbirlerinin alınması ve bu tedbirlerin sürekliliği için gerekli personel, teçhizat ve kullanıcı eğitim faaliyetlerinin de temin edilmesi gerekir.
- (7) - Tüm Kullanıcılar, BGYS politikalarına uymak ve öğrenmiş oldukları gizli kalması gereken bilgileri, sır saklama yükümlülüğü uyarınca süresiz olarak saklamakla yükümlüdür.
- (8) - BGYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında işbu yönergenin “Yaptırım ve Çeşitli Hükümler” kısmında belirtildiği şekilde işlem yapılır.
- (9) - Tüm akademik ve idari birim/bölüm yöneticileri, kendilerine bağlı en uç noktalara kadar bilgi güvenliği ile ilgili tedbirlerin alınmasını sağlamaktan birinci derecede sorumludur.

BEŞİNCİ BÖLÜM

Yetki ve Sorumluluk

Yetki ve sorumluluk

MADDE 10 – (1) Üniversitede İnternet ağının kurulum ve işletmesine ait yetki ve sorumluluk BİDB’ye aittir. BİDB, akademik, idari, eğitim ve araştırma amaçları doğrultusunda bölüm ve birimlerin bilişim kaynaklarına erişimlerini sağlamak üzere oluşturulan alt yapıyı kurmak, işletmek ve güncellemekle sorumludur. BİDB, bölüm ve birimlerde tespit edilen ana ağ erişim noktalarını kurar, bilgi işlem merkezi ile iletişimi için gerekli faaliyetlerini yürütür, bu noktalara kullanıcıların bağlanabilmesi için gerekli ağ anahtarlama cihazlarını temin eder ve yerleştirir. Sistemi teknik düzeyde planlama ve uygulama sorumluluk ve yetkisi BİDB’dedir. BİDB gereken durumlarda ve istek üzerine danışmanlık hizmeti verebilir.

(2) - Tüm Kullanıcılar, Üniversite bilişim kaynaklarını kullanarak gerçekleştirdikleri her türlü etkinlikten, kendilerine tahsis edilen Üniversite bilişim kaynağı üzerinde bulundurdıkları veya oluşturdukları her türlü kaynağın (belge, doküman, yazılım, vb.) içeriğinden, kaynağın kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden, ilgili kaynağın kullanım kurallarına, kanun ve yönetmeliklere karşı sorumludur.

(3) - Komisyon, Üniversite bilişim kaynakları kullanımı hakkında genel politika ve prosedürleri belirler, bunları gelişen teknolojinin öngördüğü biçimde sürekli olarak değerlendirir ve gerekli değişiklikleri hayata geçirir. Bu tür değişiklikler yapıldığında genel duyuru mekanizmaları ile kullanıcılar bilgilendirilir.

(4) - Komisyon tarafından BGYS kapsamında hazırlanan politika ve prosedürlere tüm kullanıcılar uymak zorundadır.

ALTINCI BÖLÜM

Politikaların Hazırlanması ve Uygulanması

Politikaların Hazırlanması ve Uygulanması

MADDE 11 - (1) BGYS politika ve prosedürleri, Komisyon tarafından ilgili yasalara aykırı olmayacak şekilde ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standartlarına uygun olacak şekilde hazırlanır.

- (2) - Hazırlanan politikalar, BİDB web sayfasında yayımlanır ve hem personele hem de öğrencilere duyurulur.
- (3)- Hazırlanan politikalar, planlanan zaman aralıklarında veya teknik gereklilikler ortaya çıktığında uygunluğu, elverişliliği ve etkinliğinin sürekliliğini belirlemek amacıyla BİDB bünyesinde oluşturulacak çalışma grupları tarafından kontrol edilir. Komisyon tarafınca gerek görülmesi halinde çalışma gruplarına BİDB çalışanlarına ilave olarak kurumun istatistik, insan kaynakları, kalite, hukuk ve fiziksel güvenlikten sorumlu birimleri ile gerekli görülecek diğer personel de katılabilir.
- (4) - Politikaların yeniden bir bütün olarak yayınlanmasını gerektirmeyen küçük çaplı değişiklikler, değişiklik eki olarak hazırlanır. Değişiklik ekleri, dokümanların yürürlükteki sürümleri üzerine işlenmek suretiyle takip edilir.
- (5) - Politikalarda önemli ölçüde değişiklik yapılmasını gereken durumlarda, yeni sürümler bir bütün olarak yayımlanır.
- (6) - Konya Teknik Üniversitesi bilişim alt yapısını kullanan tüm kullanıcılar ilgili politika ve prosedürlerde belirtilen kuralları bilmeli ve bu kurallara uymalıdır.
- (7) - BİDB çalışanları, BGYS kapsamında belirlenen politika ve prosedürlere göre hareket ederler. Bu politika ve prosedürlere uymayan talepler yerine getirilmez.
- (8)- Kullanıcılar, ilgili kanunlara, politikalar kapsamında belirtilen esaslara ve TÜBİTAK ULAKBİM kullanım politikası esaslarına uymak kaydıyla, bilişim kaynaklarını esas kullanıcı veya diğer kullanıcı tanımları ve yetkileri çerçevesinde kullanma ve belirtilen hizmetleri alma hakkına sahiptir.

YEDİNCİ BÖLÜM

Üst Yönetimin Taahhüdü

Üst Yönetimin Taahhüdü

MADDE 12 – (1) Tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan BGYS’ye uyulması, sistemin verimli şekilde çalışması ve bilgi güvenliği farkındalık programları düzenlenmesi için, imkânlar dâhilinde, gerek duyulan kaynakların tahsis edilmesini

- (2) - BGYS’nin etkinliğini, sürekli iyileştirilmesini ve bunun tüm personel tarafından anlaşılmasının sağlanmasını,
 - (3) - Tüm personelimizin ve üçüncü tarafların BGYS’ye katılımını ve uyumunu sağlamak için bilinçlendirici ve yönlendirici faaliyetler planlamasının teşvik edilmesini,
 - (4) - BGYS özelinde hedefler belirlemeyi ve belirli dönemlerde uygunluklarını değerlendirerek, BGYS kapsamında risk yönetiminin gerçekleştirilmesini,
 - (5) - BGYS’nin gereksinimlerinin uygun olarak karşılanmasını teminen bilginin gizlilik, bütünlük ve erişilebilirlik unsurlarının korunmasını,
 - (6) - BGYS’nin yürütülmesi için kullanılan süreç ve faaliyetlerin sürekli iyileştirilmesi amacıyla belirli aralıklarla “Yönetim Gözden Geçirme Toplantıları”na iştirak edilmesini,
 - (7) - BGYS’nin gereği olan yasal mevzuata, sözleşme gereksinimlerine ve standartlara uyumun garanti altına alınmasını ve BGYS’nin kurum kültürümüzün vazgeçilmez bir parçası olarak uygulanmasının takip edilmesini,
- taahhüt eder.

SEKİZİNCİ BÖLÜM

Üst Yönetimin Onayı

MADDE 13 - (1) Üniversite Üst Yönetimi olarak; BGYS Politikasının uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederiz.

DOKUZUNCU BÖLÜM

Yaptırım ve Çeşitli Hükümler

Yaptırım

MADDE 14 – (1) BGYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında, 657 sayılı Devlet Memurları Kanunu, 2547 sayılı Yükseköğretim Kanunu, iş sözleşmesinin ilgili hükümleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ilgili hükümleri uyarınca işlem yapılır.

(2) - BİDB, Üniversitenin tüzel kişiliğini ve güvenliğini korumak amacıyla yasalara uygun olarak kısıtlayıcı ve engelleyici önlemler alır.

(3) - BİDB, BGYS politikalarına ve ilgili diğer yönergelere uymayan kullanıcıların hesabını iptal etme veya geçici bir süreliğine dondurma, sunduğu hizmetin şeklini değiştirme veya son verme hakkına sahiptir. Ziyaretçi veya kullanıcılar bu konudaki hizmetin şeklinin değiştirilmesinden veya sona erdirilmesinden dolayı oluşabilecek bilgi kayıplarından veya sorunlardan Konya Teknik Üniversitesi hiçbir şekilde sorumlu tutulamaz.

Hüküm Bulunmayan Haller

MADDE 15 – (1) Bu Yönergede hüküm bulunmayan hallerde; ilgili mevzuat hükümleri ile Yükseköğretim Kurulu, Senato ve ilgili Yönetim Kurulu Kararları uygulanır.

Yürürlük

MADDE 16 – (1) Bu Yönerge Konya Teknik Üniversitesi Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 17 – (1) Bu Yönerge hükümlerini Konya Teknik Üniversitesi Rektörü yürütür.

Yönergenin Kabul Edildiği Senato Tarihi:21/06/2023 Sayısı:12-02