

ÇANKIRI KARATEKİN ÜNİVERSİTESİ BİLGİ VE İLETİŞİM GÜVENLİĞİ KOMİSYONU YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Yönergenin amacı; Çankırı Karatekin Üniversitesi bünyesinde bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak, siber olayların etkilerini azaltmak, iş sürekliliğini sağlamak ve özellikle milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verilerin güvenliğini sağlamak üzere asgari güvenlik tedbirlerinin belirlenmesi; ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi gereklilikleri doğrultusunda bir Bilgi ve İletişim Güvenliği Komisyonu’nun kuruluşu, görev, yetki ve sorumlulukları ile çalışma usul ve esaslarını düzenlemektir.

Kapsam

MADDE 2 – (1) Bu Yönerge, Çankırı Karatekin Üniversitesi Bilgi ve İletişim Güvenliği Komisyonu’nun kuruluşu ile çalışmasına ilişkin usul ve esasları, Üniversitenin tüm akademik ve idari birimlerini, bu birimlerde görev yapan tüm personeli, öğrencileri, misafir (üçüncü kişi) kullanıcıları ve Üniversitenin bilgi sistemlerini kullanan üçüncü taraf hizmet sağlayıcılarını kapsar.

Dayanak

MADDE 3 – (1) Bu Yönerge;

- a) 2547 sayılı Yükseköğretim Kanunu’nun 14. maddesi,
- b) 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- c) T.C. Cumhurbaşkanlığı’nın 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi,
- ç) T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi ve
- d) TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu Yönergede geçen;

- a) Üniversite: Çankırı Karatekin Üniversitesi’ni,
- b) Rektör: Çankırı Karatekin Üniversitesi Rektörü’nü,
- c) BGYS: Bilgi Güvenliği Yönetim Sistemi’ni,
- ç) BİG Rehberi: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi’ni,
- d) BİGK (Komisyon): Bilgi ve İletişim Güvenliği Komisyonu’nu,
- e) Bilgi Güvenliği Yöneticisi: Kurumsal SOME Yöneticisini,
- f) Bilgi Sistemleri Yöneticisi: Üniversitede bilgi sistemlerinin yönetiminden sorumlu Bilgi İşlem Daire Başkanı’nı,
- g) Bilgi Varlığı: Üniversitenin iş süreçleri için değeri olan, basılı veya elektronik ortamdaki her türlü veriyi, yazılımı, donanımı, altyapıyı ve personele ilişkin her türlü bilgiyi,
- ğ) İlgili Birim: Üniversite organizasyon şemasında yer alan her bir birimi,

- h) Komisyon Başkanı: Bu yönerge ile kurulan komisyona başkanlık yapacak Rektör'ün görevlendireceği Rektör Yardımcısı'nı,
- i) Koordinasyon Birimi: Bilgi İşlem Daire Başkanlığı'nı,
- j) Kurumsal SOME: Üniversitede bulunan Siber Olaylara Müdahale Ekibi'ni,
- k) Varlık: Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren; Üniversitenin iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânları,
- k) Varlık Grubu Koordinatörü: Rehber uygulama sürecinde yer alan aşamalarda bilgi birikimine danışılan ve bu aşamaları koordine eden uzman personeli, ifade eder.

İKİNCİ BÖLÜM

Komisyonun Oluşumu, Görev, Yetki ve Sorumlulukları

Komisyonun Oluşumu

MADDE 5 – (1) Bilgi ve İletişim Güvenliği Komisyonu, Rektör tarafından görevlendirilen Rektör Yardımcısı başkanlığında aşağıdaki üyelerden oluşur:

- Bilgi Sistemleri Yöneticisi (Bilgi İşlem Daire Başkanı)
 - Bilgi Güvenliği Yöneticisi (Kurumsal SOME Yöneticisi)
 - Varlık Grubu Koordinatörü (Bilgi İşlem Daire Başkanlığında görevli uzman bir personel)
 - Genel sekreter
 - Öğrenci İşleri Daire Başkanı
 - Personel Daire Başkanı
 - Üniversitede görevli akademik bir personel (Bilgi ve İletişim Güvenliği Uzmanı)
 - Danışman olarak Rektör'ün belirleyeceği bir Üniversite iç denetim personelinin oluşur.
- (2) Komisyon üyeleri Rektör tarafından görevlendirilir. Komisyon üyelerinin görev süresi 3 (üç) yıldır. Komisyon üyelerinin görev süreleri sona erdiğinde yeniden aynı usulle görevlendirilebilir.

Komisyonun Görev, Yetki ve Sorumlulukları

MADDE 6 – (1) Komisyonun görev ve yetkileri şunlardır:

- BİG Rehberi ve ISO 27001 standardına uygun olarak Üniversitenin Bilgi ve İletişim Güvenliği sistemini kurmak, politikaları belirlemek, uygulamaya yönelik kararlar almak ve sürdürülebilirliğini sağlamak.
- Üniversite bilgi ve iletişim güvenliği sisteminin idari ve akademik birimler düzeyinde kurulması, sürdürülmesi ve iyileştirilmesi için gerekli koordinasyonu sağlamak ve öneriler geliştirmek.
- Bilgi güvenliği risk yönetimi süreçlerini yönetmek, risk işleme planlarını onaylamak ve kabul edilebilir risk seviyelerine karar vermek.
- Bilgi ve İletişim Güvenliği Sistemi kapsamında yapılan inceleme, araştırma, denetim faaliyetleri sonucunda tespit edilen bulgulara ilişkin düzeltici/iyileştirici kararları almak; uygulamalara ilişkin değerlendirmelerde bulunmak, bilgi ve iletişim güvenliği denetiminin planlandığı şekilde yapılabilmesi için gerekli kaynakları sağlamak.
- Gerçekleşen önemli bilgi/veri güvenliği ihlal olaylarını değerlendirmek ve bu olayların tekrarlanmasını önleyecek düzeltici/iyileştirici kararları almak.
- Bilgi güvenliği denetimlerinin yapılmasını sağlamak, denetim raporlarını ve bulgularını değerlendirerek gerekli aksiyonların alınmasına karar vermek.
- Gerekli görülen durumlarda Komisyon bünyesinde alt çalışma grupları veya ekipler oluşturmak ve bu ekiplerin çalışma usul ve esaslarını belirlemek.

ÜÇÜNCÜ BÖLÜM

Koordinasyon Birimi Görev ve Sorumlulukları

MADDE 7- (1) Koordinasyon Birimi, Üniversite Bilgi İşlem Daire Başkanlığı'dır. Koordinasyon Birimi'nin görevleri şunlardır:

- a) Üniversitede bilgi ve iletişim güvenliği sistemine göre komisyon tarafından alınan kararların uygulanmasını sağlamak,
- b) Mevcut iş süreçlerinin tespiti, izlenmesi ve iyileştirilmesini sağlamak,
- c) Bilgi ve iletişim güvenliği sistemlerine yönelik belge altyapısını oluşturmak,
- ç) Bilgi ve İletişim Güvenliği Komisyonu tarafından belirlenen usul ve esaslar çerçevesinde alınan kararlara ilişkin yürütülecek çalışmaları yapmak,
- d) Üniversite genelinde bilgi ve veri güvenliği ile ilgili koordinasyonu sağlamak, planlama-programlama yapmak, Bilgi ve İletişim Güvenliği Komisyonuna destek sağlayarak, işleyişe yönelik hizmetleri sunmaktır.

DÖRDÜNCÜ BÖLÜM

Çalışma Usul ve Esasları

MADDE 8– (1) Bilgi ve İletişim Güvenliği Komisyonu aşağıda belirtilen esaslar doğrultusunda çalışır:

- a) Komisyon, Başkanın belirleyeceği tarihlerde ve çağrısı üzerine yılda en az bir kez toplanır. Başkan veya üyeler olağan toplantılar dışında olağanüstü gündem ile her zaman toplantı yapılmasını isteyebilirler.
- b) Komisyon kararlarının ilgili birim yöneticileri tarafından yürütülmesi esastır. İlgili birim yöneticileri tarafından Bilgi ve İletişim Güvenliği Sistemi çalışmaları ve sonuçları Koordinasyon Birimine iletilir ve Koordinasyon Birimi tarafından Komisyona raporlanır. Komisyon, sunulan raporları değerlendirmek suretiyle alacağı kararları Rektör'ün onayına sunar.
- c) Mutad toplantıların gündemi, yeri ve tarihi, Komisyon Başkanı tarafından belirlenir.
- ç) Tüm duyuru ve yazışmalar Bilgi İşlem Daire Başkanlığı tarafından yapılır.
- d) Bilgi ve İletişim Güvenliği Komisyonu, üye tam sayısının salt çoğunluğuyla toplanır ve toplantıya katılanların oy çokluğu ile karar alır. Oyların eşit olması durumunda Komisyon Başkanının oyu yönünde karar alınmış sayılır.
- e) Komisyonun ofis, personel destek, danışmanlık ve eğitim hizmetleri, Koordinasyon Birimi tarafından yürütülür.

BEŞİNCİ BÖLÜM

Bilgi ve İletişim Güvenliği Sistemi Uygulama Süreci

MADDE 9 – (1) Bilgi ve İletişim Güvenliği Sistemi Uygulama Süreci planlama, uygulama, kontrol etme ve önlem alma ile değişiklik yönetimi alt süreçlerinden oluşmaktadır:

(a) Planlama:

- 1) Varlık gruplarının belirlenmesi,
- 2) Varlık gruplarının kritiklik derecelendirmesinin belirlenmesi,

- 3) Varlık gruplarının mevcut durumunun analizi ve boşluk analizinin yapılması,
- 4) Sistem uygulama yol haritasının hazırlanması faaliyetleri yürütülür.

(b) Uygulama:

- 1) Tedbirlerin uygulanması,

(c) Kontrol etme ve önlem alma:

- 1) Sistem uygulama yol haritasının izlenmesi ve kontrol edilmesi,
- 2) Bilgi ve iletişim güvenliği denetiminin yapılması,

(ç) Değişiklik Yönetimi:

- 1) Bilgi ve iletişim güvenliği sistemi değişikliklerinin yönetilmesi,
- 2) Varlık gruplarının değişikliklerinin yönetilmesi,

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Hüküm Bulunmayan Haller

MADDE 10 – (1) Bu Yönerge'de hüküm bulunmayan hallerde ilgili mevzuat ile T.C. Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve ilgili mevzuat hükümleri uygulanır.

Yürürlük

MADDE 11 – (1) Bu Yönerge, Üniversite Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 12 – (1) Bu Yönerge hükümlerini Çankırı Karatekin Üniversitesi Rektörü yürütür.