ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ

BİLGİ VE İLETİŞİM GÜVENLİĞİ KOMİSYONU YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar

Amaç

MADDE 1 - (1) Bu Yönergenin amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle varlığın gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi veya verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için faaliyet gösterecek Komisyonun kuruluş ve çalışmasına ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönerge, Ankara Yıldırım Beyazıt Üniversitesi Bilgi ve İletişim Güvenliği Komisyonunun kuruluşu ile çalışmasına ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönerge; 4/11/1981 tarihli ve 2547 sayılı Yükseköğretim Kanununun 14 üncü maddesi, 6 Temmuz 2019 tarihli ve 30823 Sayılı Resmi Gazetede yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ile 10.07.2020 tarihli T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu yönergede geçen;

a) Bağımsız Dış Değerlendirme Kuruluşları: Yurt içinde veya yurt dışında dış değerlendirme ve faaliyetleri gösteren kurum ve kuruluşları,

b) Bilgi ve İletişim Güvenliği Birimi: Ankara Yıldırım Beyazıt Üniversitesi Rektörlüğü bünyesinde yer alan, Bilgi ve İletişim Güvenliği Sisteminin uygulanmasında Komisyonun çalışmalarını yürüten, ilgili raporlamaları yapan, Üniversite birimleriyle iletişimi sağlayan birimi,

c) Bilgi Güvenliği Yöneticisi: Üniversitede bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu Rektör Yardımcısını,

ç) Bilgi Sistemleri Yöneticisi: Üniversitede bilgi sistemlerinin yönetiminden sorumlu Bilgi İşlem Daire Başkanını,

d) Bilgi ve İletişim Güvenliği Sistemi: Üniversitenin bilgi ve iletişim güvenliği rehberi standartları ile uyumlu bilgi ve iletişim güvenliği süreçlerinin tam olarak yerine getirilmesi için yapılan tüm planlı ve sistemli işlemleri,

e) Birim: Üniversite organizasyon şemasında yer alan her bir birimi,

f) Dış Denetim Personeli: Bilgi ve İletişim Güvenliği Sistemi uygulama sürecinin ve güvenlik tedbirlerinin Üniversitede uygulanıp uygulanmadığını denetleyen üçüncü taraf denetçileri,

g) Dış Paydaş: Dış denetim personelini, bağımsız dış değerlendirme kuruluşlarını,

h) İç Denetçi: Üniversitede iç denetimi gerçekleştiren personeli,

ı) İç Paydaş: Rektör, bilgi güvenliği yöneticisi, bilgi sistemleri yöneticisi, iç denetçi, ilgili birim yöneticisi, ilgili birim uzman personeli, varlık grubu koordinatörü ve Kurumsal SOME yöneticisini,

i) Birim Uzman Personeli: Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alan ve her bir birimden atanan birim yetkilisini,

j) Birim Yöneticisi: Üniversitede, rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim yöneticisini (Dekan/Fakülte Sekreteri, Daire Başkanı, Koordinatörler, Yüksekokul-MYO-Enstitü Müdürü/Sekreteri, Araştırma ve Uygulama Merkezi Müdürü/Hastaneler Başmüdürü),

k) Komisyon: Ankara Yıldırım Beyazıt Üniversitesi Bilgi ve İletişim Güvenliği Komisyonunu,

l) Kurumsal SOME Yöneticisi: Üniversitede bulunan siber olaylara müdahale ekibinin yöneticisini,

m) Rehber: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı Bilgi ve İletişim Güvenliği Rehberini,

n) Rektör: Ankara Yıldırım Beyazıt Üniversitesi Rektörünü,

o) Senato: Ankara Yıldırım Beyazıt Üniversitesi Senatosunu,

ö) Üniversite: Ankara Yıldırım Beyazıt Üniversitesini,

p) 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,

r) Varlık Grubu Koordinatörü: Rehber uygulama sürecinde yer alan aşamalarda bilgi birikimine danışılan ve bu aşamaları koordine eden uzman personeli,

ifade eder.

İKİNCİ BÖLÜM

Üniversite Bilgi ve İletişim Güvenliği Komisyonunun Oluşturulması,

Yapısı, Görev, Yetki ve Sorumlulukları ile Çalışma Esasları

Komisyonun oluşturulması ve yapısı

MADDE 5 - (1) Bilgi ve İletişim Güvenliği Komisyonu; Rektör, Bilgi Güvenliği Yöneticisi, Bilgi Sistemleri Yöneticisi, Varlık Grubu Koordinatörü, Kurumsal SOME Ekibinin Yöneticisi, Yapı İşleri ve Teknik Daire Başkanı, Personel Daire Başkanı ve Rektörün belirleyeceği Üniversite iç denetim personelinden oluşur.

(2) Komisyonun başkanı Rektördür. Rektörün bulunmadığı zamanlarda, görevlendirdiği rektör yardımcısı komisyona başkanlık eder.

(3) Rektörlüğün uygun gördüğü personelin komisyon toplantısına katılması istenebilir.

Komisyonun görev, yetki ve sorumlulukları:

MADDE 6 - (1) Komisyonun görev, yetki ve sorumlulukları şunlardır:

a) Rehbere uygunluğun değerlendirilmesi, izlenmesi ve planlanması amacıyla Üniversitenin Bilgi ve İletişim Güvenliği Sistemini oluşturmak ve sürdürülebilirliğini sağlamak,

b) Bilgi ve İletişim Güvenliği Sistemi uygulamalarının Rehbere uygun olarak yürütülmesini sağlamak,

c) Üniversite Bilgi ve İletişim Güvenliği Sisteminin birimler düzeyinde kurulması, sürdürülmesi ve iyileştirilmesi için gerekli koordinasyonu sağlamak ve öneriler geliştirmek,

ç) Gerekli görülen durumlarda Komisyon bünyesinde alt ekipler oluşturmak, çalışma usul ve esaslarını belirlemek,

d) Bilgi ve İletişim Güvenliği Sisteminin uygulanmasında katılımcılığa, kaynakları etkin ve verimli kullanmaya, süreçleri iyileştirmeye dayalı bir kurum kültürünün geliştirilmesini ve yaygınlaştırılmasını sağlamak,

e) Bilgi ve İletişim Güvenliği Sisteminin etkinliğini artırıcı politikalar belirlemek ve uygulamaya yönelik kararlar almak,

f) 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 yapılması için gerekli kaynakları sağlamaktır.

Çalışma esasları

MADDE 7 – (1) Bilgi ve İletişim Güvenliği Komisyonu aşağıda belirtilen esaslar doğrultusunda çalışır:

a) Komisyon, Başkanın belirleyeceği tarihlerde ve çağrısı üzerine en az yılda bir kez toplanır. Başkan veya üyeler olağan toplantılar dışında olağanüstü gündem ile her zaman toplantı isteyebilir.

b) Komisyon kararlarının ilgili birim yöneticileri tarafından yürütülmesi esastır. İlgili birim yöneticileri tarafından yapılan Bilgi ve İletişim Güvenliği Sistemi çalışmaları ve sonuçları Bilgi ve İletişim Güvenliği Birimine iletilir ve Birim tarafından Komisyona raporlanır. Komisyon; sunulan raporları, niteliğine göre karar almak veya Senatoya sunmak suretiyle değerlendirir.

c) Bilgi ve İletişim Güvenliği denetiminin yapılması sonucunda çıkan bulgular, İç Denetim Birimi tarafından Bilgi ve İletişim Güvenliği Komisyonuna iletilir. Komisyon tarafından bulgular ile ilgili sorumlular belirlenir. Bulgular; Bilgi ve İletişim Güvenliği Birimi tarafından, Komisyonun belirlediği Üniversite Organizasyon Şemasındaki ilgili birimlere faaliyetlerin yerine getirilmesi için iletilir. Birimlerden gelen bulguların kapatılmasına yönelik faaliyet sonuçlarını Bilgi ve İletişim Güvenliği Komisyonu onayı ile İç Denetim Birimine raporlar.

ç) Mutat toplantıların gündemi, yeri ve tarihi; Komisyon Başkanı tarafından belirlenir.

d) Tüm duyuru ve yazışmalar Bilgi ve İletişim Güvenliği Birimi tarafından yapılır.

e) Bilgi ve İletişim Güvenliği Komisyonu, üye tam sayısının salt çoğunluğuyla toplanır ve toplantıya katılanların salt çoğunluğuyla karar alır. Oyların eşit olması durumunda Komisyon Başkanının oyu yönünde karar alınmış sayılır.

f) Komisyonun ofis, personel destek, danışmanlık ve eğitim hizmetleri, Bilgi ve İletişim Güvenliği Birimi tarafından yürütülür.

ÜÇÜNCÜ BÖLÜM

Bilgi ve İletişim Güvenliği Biriminin Tanımı, Görev ve Sorumlulukları

Bilgi ve İletişim Güvenliği Biriminin tanımı

MADDE 8 - (1) Bilgi ve İletişim Güvenliği Birimi, Üniversitenin Bilgi ve İletişim Güvenliği sisteminin uygulanmasında Komisyonun çalışmalarını yürütme, ilgili raporlamaları yapma, Üniversite birimleriyle iletişimi sağlama faaliyetlerini takip eder.

Bilgi ve İletişim Güvenliği Biriminin görev ve sorumlulukları

MADDE 9 - (1) Bilgi ve İletişim Güvenliği Biriminin görevleri şunlardır:

a) Üniversitede bilgi ve iletişim güvenliği sistemine göre komisyon tarafından alınan kararların uygulanmasını sağlamak,

b) Bilgi ve İletişim Güvenliği Sistemi Uygulama Sürecindeki faaliyetlerin tespiti, izlenmesi ve iyileştirilmesini sağlamak,

c) Bilgi ve iletişim güvenliği sistemlerine yönelik belge altyapısını oluşturmak,

ç) Bilgi ve iletişim 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 iletişim güvenliği komisyonuna destek sağlayarak, süreçlerin uygulanması hizmetlerini sunmaktır.

DÖRDÜNCÜ BÖLÜM

Bilgi ve İletişim Güvenliği Sistemi Uygulama ve Denetim Süreci

Bilgi ve İletişim Güvenliği Sistemi uygulama süreci

MADDE 10 – (1) Bilgi ve İletişim Güvenliği Sistemi Uygulama Süreci; planlama, uygulama, kontrol etme ve önlem alma ile değişiklik yönetimi alt süreçlerinden oluşmaktadır.

a) Planlama sürecinde;

1) Varlık gruplarının belirlenmesi,

2) Varlık gruplarının kritiklik derecesinin belirlenmesi,

3) Varlık gruplarının mevcut durumunun analizi ve boşluk analizinin yapılması,

4) Boşluk analizi sonucunda uygulanması gereken ilave tedbirler kapsamındaki herhangi bir gereksinimi; üst yönetim tarafından onaylanmış teknik kısıtlamalardan ve iş gereksinimlerinden dolayı Rehberde tanımlandığı şekli ile karşılayamaması durumunda uygulanacak telafi edici kontrollerin belirlenmesi,

5) Rehber uygulama yol haritasının hazırlanması,

faaliyetleri yürütülür.

b) Uygulama sürecinde;

1) Güvenlik tedbirlerinin uygulanması faaliyeti yürütülür.

c) Kontrol etme ve önlem alma sürecinde;

1) Bilgi ve İletişim Güvenliği Rehberi uygulama yol haritasının ilerleme durumlarının takibi ve kontrollerin yapılması, hazırlanan plandan sapmaların tespit edilerek gerekli önlemlerin alınması ile ilgili çalışmaların yürütülmesi,

2) Rehber güvenlik tedbirlerinin uygulanmasına ilişkin, Üniversite İç Denetim Birimi tarafından, Üniversitenin bilgi ve iletişim güvenliği iyileştirmelerini içerecek şekilde yapılan denetim sonucunda oluşturulan rapora ilişkin çalışmaların koordinasyonu,

faaliyetleri yürütülür.

ç) Değişiklik yönetimi sürecinde;

1) Kurumsal ihtiyaçlar ve gelişmeler dikkate alınarak varlık grupları ile uygulama ve teknoloji ya da sıkılaştırma tedbirleri kapsamında gerçekleşecek bir değişiklik tespit edildiğinde tekrar planlama yapılarak rehber yol haritasının güncellenmesi,

2) Cumhurbaşkanlığı tarafından Rehberin güncellendiği durumlarda sürecin tamamının gözden geçirilmesi ve gerekli çalışmaların yapılması,

faaliyetleri yürütülür.

Denetim süreci ile denetim raporunun kapsamı ve takvimi

MADDE 11 – (1) Üniversite İç Denetim Birimi, Üniversite Bilgi ve İletişim Güvenliği Komisyonu ile iş birliği içinde yıllık olarak bir denetim süreci yürütür. Süreç sonunda Üniversite İç Denetim Birimi Üniversitenin bilgi ve iletişim güvenliği iyileştirmelerini de içerecek şekilde denetim raporunu hazırlar.

(2) Denetim değerlendirme konuları, bilgi ve iletişim güvenliği rehberi güvenlik tedbirleri ile sınırlıdır.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Bilgi ve İletişim Güvenliği Sistemi oluşturma çalışmaları kapsamında yapılan harcama ve görevlendirmeler

MADDE 12 – (1) Bu Yönerge kapsamında, üniversite tarafından gerçekleştirilecek çalışmalara ilişkin her türlü harcama, üniversitenin bütçesine ilgili konuda tahsis edilecek ödenekle karşılanır.

Hüküm bulunmayan haller

MADDE 13 - (1) Bu Yönergede hüküm bulunmaması hâlinde 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ile T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi hükümleri uygulanır.

Yürürlük

MADDE 14 - (1) Bu Yönerge, Senatoda kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 15 - (1) Bu Yönerge hükümlerini Rektör yürütür.