T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
BİLGİ VE İLETİŞİM GÜVENLİĞİ KOMİSYONU YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak, Tanımlar

Amaç

MADDE 1 - (1) Bu Yönerge'nin 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/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, Çanakkale Onsekiz Mart Üniversitesi Bilgi ve İletişim Güvenliği Komisyonunun kuruluşu ile çalışmasına ilişkin usul ve esaslara ilişkin düzenlemeleri kapsar.

Dayanak

MADDE 3 - (1) Bu Yönerge hazırlanmasında; 2547 sayılı Kanunun 14. Maddesi ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı'nın 10.07.2020 tarih ve 2020/1.0 sürüm no.lu Bilgi ve İletişim Güvenliği Rehberi'ne dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönerge'de geçen;

a) Bağımsız Dış Değerlendirme Kuruluşları: Yurt içinde veya yurt dışında dış değerlendirme ve faaliyetleri gösteren kurum ve kuruluşları,
b) Bilgi Güvenliği Yöneticisi: Bilgi İşlem Daire Başkanlığından sorumlu Rektör Yardımcısını,
c) Bilgi Sistemleri Yöneticisi: Üniversitede bilgi sistemlerinin yönetiminden sorumlu Bilgi İşlem Daire Başkanını,
ç) 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,
d) Birim: Üniversitede bulunan ve kurulacak akademik ve idari her bir birimi,
e) Birim Varlık Grubu Koordinatörü: Rehber uygulama sürecini ilgili birimde koordine eden personeli
f) Dış Denetim Personeli: Rehber uygulama sürecinin ve güvenlik tedbirlerinin Üniversitede uygulanıp uygulanmadığını denetleyen üçüncü taraf denetçileri,
g) Dış Denetim Personeli: Sistem uygulama sürecinin ve güvenlik tedbirlerinin Üniversitede uygulanıp uygulanmadığını denetleyen üçüncü taraf denetçileri,

ğ) Dış Paydaş: Üniversite dışından bilgi ve iletişi güvenliği faaliyetleri ile ilgili faaliyetlere katılım sağlayan herkesi,
h) İç Denetçi: Üniversitede iç denetimi gerçekleştiren personeli,
ı) İç Paydaş: Rektör, bilgi güvenliği yöneticisi, bilgi sistemleri yöneticisi, iç denetçi, ilgili birim yöneticileri, ilgili birim uzman personeli, varlık grubu koordinatörünü,
i) İlgili Birim Uzman Personelleri: Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim personelini,
j) İlgili Birim Yöneticileri: Üniversitede, rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim yöneticilerini (Dekan/Fakülte Sekreteri, Daire Başkanı, Koordinatörler, Yüksekokul-MYO-Enstitü Müdürü/sekreteri, Araştırma ve Uygulama Merkezi/TTO Müdürü/Hastaneler Başmüdürü),
k) Komisyon: Çanakkale Onsekiz Mart Üniversitesi Bilgi ve İletişim Güvenliği Komisyonunu,
l) Koordinasyon Birimi: Bilgi İşlem Daire Başkanlığını,
m) Kurumsal SOME Yöneticisi: Üniversitede bulunan siber olaylara müdahale ekibinin yöneticisini,
n) Rehber : T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı'nın Bilgi ve İletişim Güvenliği Rehberini,
o) Rektör : Çanakkale Onsekiz Mart Üniversitesi Rektörünü,
ö) Senato: Çanakkale Onsekiz Mart Üniversitesi Senatosunu,
p) Üniversite: Çanakkale Onsekiz Mart Üniversitesini,
r) 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,
s) Varlık Grubu Koordinatörü: Rehber uygulama sürecinde yer alan aşamalarda bilgi birikimine danışılan ve bu aşamaları koordine eden üst personeli,
ş) Varlık Grubu Birim Koordinatörü: Rehber uygulama sürecinde yer alan, Üniversitenin ilgili birimlerinde görevli olan, bilgi birikimine danışılan ve aşamalarını kontrol eden 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) Üniversite Bilgi ve İletişim Güvenliği Komisyonunun başkanı Rektördür, Rektörün bulunmadığı zamanlarda, görevlendireceği rektör yardımcısı komisyona başkanlık eder.

(2) Rektör tarafından görevlendirilen komisyon;

a) Bilgi İşlem Daire Başkanlığından sorumlu Rektör yardımcısı (Bilgi Güvenliği Yöneticisi olarak),
b) Bilgi İşlem Daire Başkanı (Bilgi Sistemleri Yöneticisi),

c) Bilgi İşlem Daire Başkanlığında görevli uzman personel (Varlık Gurubu Koordinatörü),

ç) Üniversitede görevli akademik bir personel (Bilgi ve İletişim Güvenliği Uzmanı)

d) Rektörün belirleyeceği Üniversite iç denetim personelinden oluşur.

(3) Komisyon üyelerinin görev süresi 2 yıldır. Üyenin görev süresi dolmadan üyeliğin boşalması halinde, yeni göreve atanan kişi kalan süreyi doldurur.

Sorumluluk Atama Matrisi

MADDE 6 - (1) Tablo 1'de Sorumluluk Atama Matrisinin rollerine ilişkin kısaltmaların açıklamaları yer almaktadır

Tablo 1. Sorumluluk Atama Matrisi Rolleri Açıklamaları

Kısaltma	Açıklaması
S	Sorumlu: Görevi gerçekleştiren personel
O	Onaylayan: Görevi durdurabilen, devam ettirebilen, son kararı verebilen ve hesap veren personel
D	Danışılan: Görev yapılmadan önce bilgisine başvurulması gereken personel
B	Bilgilendirilen: Görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel

(2) Tablo 2'de roller; ilgili personelin üstlendiği veya o kişiye atanan görev olarak ifade edilmektedir. Alt süreçler doğrultusunda gerçekleştirilecek çalışmalar ise faaliyet olarak tanımlanmakta olup, her bir rolün faaliyetler özelinde tanımlanan sorumluluk ve yetki alanları yer almaktadır.

Tablo 2. Bilgi ve İletişim Güvenliği Komisyonu için
Sorumluluk Atama Matrisi

No.	FAALİYET ADI	ROL ADI										
		İÇ PAYDAŞLAR						DIŞ PAYDAŞLAR				
		Kurumun En Üst Düzey Yöneticisi	Bilgi Güvenliği Yöneticisi	Bilgi Sistemleri Yöneticisi	İç Denetçi	İlgili Birim Yöneticileri	İlgili Birim Uzman Personeli	Varlık Grubu Koordinatörü	Dış Denetim Personeli	Dijital Dönüşüm Ofisi	Bağlı/İlgili/İlişkili Üst Kurum	İlgili Düzenleyici ve Denetleyici Kurum	Teknik Danışman
1	Varlık Gruplarının Belirlenmesi	O	S	S	B	S	S	D					D
2	Varlık Grubu Kritiklik Derecesinin Belirlenmesi	O	S	S		S	S	D					D

3	Mevcut Durum ve Boşluk Analizinin Yapılması	O	S	S	B	S	S	D					D
4	Sistem Uygulama Yol Haritasının Belirlenmesi	O	S	S		B	S	D					D
5	Sistem Uygulama Yol Haritasının Hayata Geçirilmesi	O	S	S		S	S	B					
6	Bilgi ve İletişim Güvenliği Denetiminin Yapılması	O	B	B	S	B		D	S	S,B	B	B	
7	Sistem Uygulama Yol Haritasının İzlenmesi ve Kontrol Edilmesi	O	S	S		S	S	B					D
8	Bilgi ve İletişim Güvenliği Sistem Değişikliklerinin Yönetilmesi	O	S	S	B	S	S	D					D
9	Varlık Gruplarının Değişikliklerinin Yönetilmesi	O	S	S	B	S	S	D					D

Komisyonun görev, yetki ve sorumlulukları:

MADDE 7 - (1) T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin yayınladığı Bilgi ve İletişim Güvenliği Rehberi'ne uygunluğunun değerlendirilmesi, izlenmesi ve planlanması amacıyla Üniversitenin bilgi ve iletişim güvenliği sistemini kurmak ve yürütmek,

(2) Rehberin Üniversiteye özgü uygulanabilir maddelerini tespit etmek ve değerlendirmesini yapmak,

(3) Bilgi ve iletişim güvenliği sistemi kapsamındaki çalışmaları Rehber çerçevesinde yürüterek senatoya sunmak,

(4) Kurumsal denetim programı için gerekli hazırlıkları yapmak, süreçle ilgili iç ve dış paydaşları bilgilendirmek,

(5) Üniversite bilgi ve iletişim güvenliği sisteminin birimler düzeyinde kurulması, sürdürülmesi ve iyileştirilmesi için gerekli koordinasyonu sağlamak ve öneriler geliştirmek,

(6) Birimlerde bilgi ve iletişim güvenliği sistemine yönelik yürütülen/yapılacak çalışmalara gerekli desteği sağlamak, gerekli görülen durumlarda birimler bünyesinde bilgi ve iletişim güvenliği ekibi oluşturulması kararı alarak oluşturulan ekibe komisyon üyeleri arasından lider tayin etmek, ekiplerin çalışma usul ve esaslarını belirlemek,

(7) Bilgi ve iletişim güvenliği sisteminin uygulanmasında katılımcılığa, kaynakları etkin ve verimli kullanmaya, süreçleri iyileştirmeye dayalı bir kurum kültürünün geliştirilmesini ve yaygınlaşmasını sağlamak,

(8) Bilgi ve iletişim güvenliği sisteminin etkinliğini artırıcı politikalar belirlemek ve uygulamaya yönelik kararlar almak,

(9) Bilgi ve iletişim güvenliği sistemi kapsamında yapılan inceleme, araştırma, denetim faaliyetleri sonucu veya dış denetim personeli tarafından yapılan denetimde tespit edilen uygunsuzluklara ilişkin düzeltici/iyileştirici kararları almak, uygulamalara ilişkin değerlendirmelerde bulunmak, kurumsal denetimin planlandığı şekilde yapılması için gerekli kaynakları sağlamak ve sonuçlarını izlemek,

Çalışma Esasları

MADDE 8 – (1) 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 isteyebilir. Komisyon faaliyetlerinin ilgili birim yöneticileri tarafından yürütülmesi esastır. İlgili birim yöneticileri tarafından yapılan çalışmalar ve sonuçları komisyona rapor halinde sunulur. Komisyon, sunulan raporları niteliğine göre karar almak veya Senatoya sunmak suretiyle değerlendirir.

(2) Komisyon aşağıda belirtilen esaslar doğrultusunda çalışır:

a) Olağan toplantıların gündemi yeri ve tarihi Komisyon Başkanı tarafından belirlenir.

b) Tüm duyuru ve yazışmalar Bilgi İşlem Daire Başkanlığı tarafından yapılır.

c) Komisyon, üye tam sayısının salt çoğunluğuyla toplanır ve toplantıya katılanların oy çokluğu ile karar alır. Oyların eşit olması durumunda başkanın oyu yönünde karar alınmış sayılır.

ç) Komisyonun ofis, personel destek, danışmanlık ve eğitim hizmetleri, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.

ÜÇÜNCÜ BÖLÜM
Koordinasyon Birimi Görev ve Sorumlulukları

MADDE 9 - (1) Koordinasyon Birimi, Üniversite Bilgi İşlem Daire Başkanlığı'dır. Koordinasyon Biriminin 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 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 Süreci

MADDE 10 – (1) Uygulama Süreci Şekil 1'de gösterildiği gibi 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,

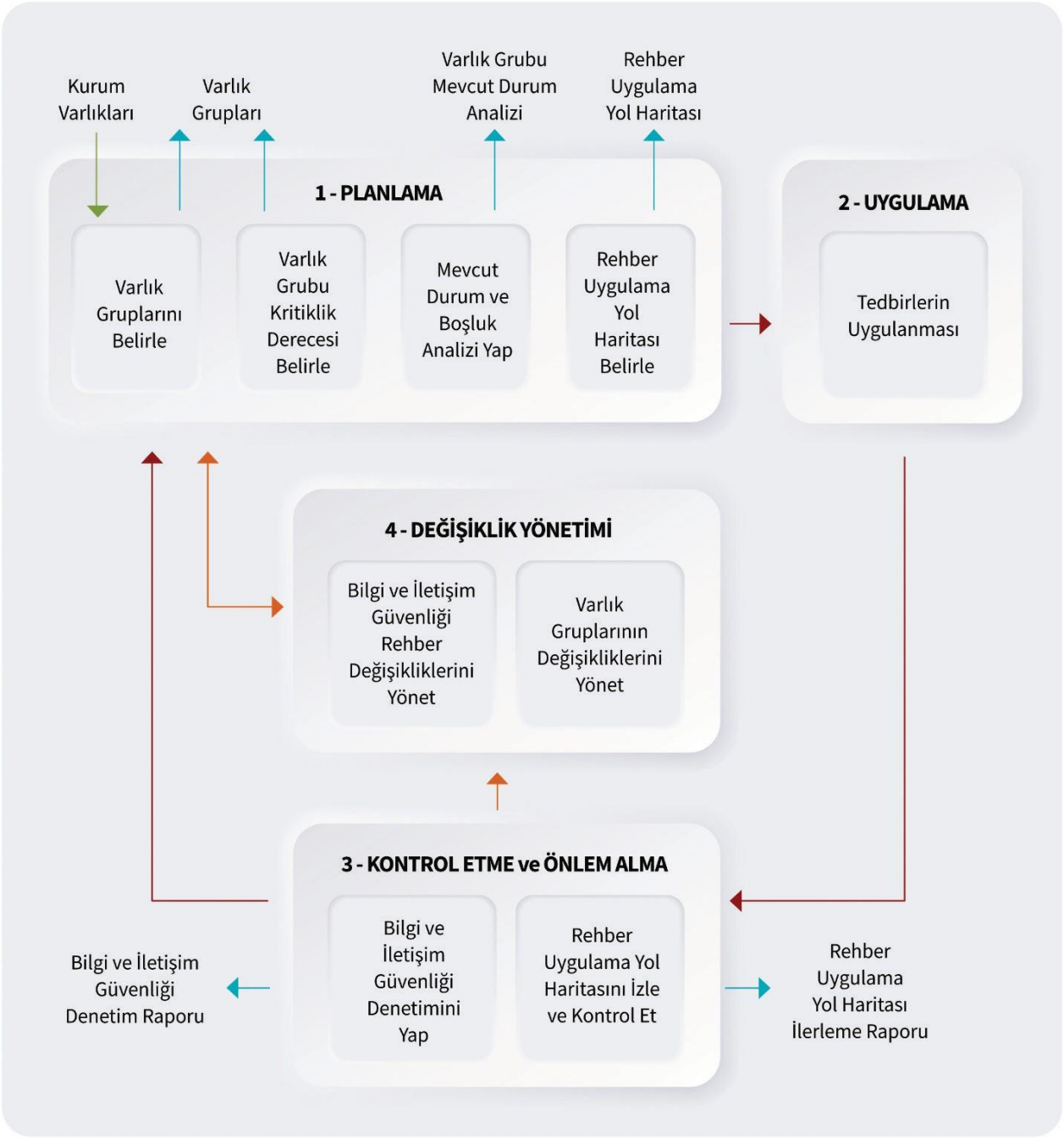
2) Bilgi ve iletişim güvenliği denetiminin yapılması,

(ç) Değişiklik Yönetimi:

1) Bilgi ve iletişim güvenliği sistemi değişikliklerinin yönetilmesi,

2) Varlık gruplarının değişikliklerinin yönetilmesi,

Şekil 1: Bilgi ve İletişim Güvenliği Sistemi Uygulama Süreci görseli



BEŞİNCİ BÖLÜM
Denetim Süreci ile Denetim Raporunun Kapsamı ve Takvimi

MADDE 11 – (1) Üniversite Bilgi ve İletişim Güvenliği Komisyonu, Bilgi İşlem Daire Başkanlığının koordinasyonunda yıllık olarak bir denetim süreci yürütür, süreç sonunda denetim raporunu, Üniversitenin bilgi ve iletişim güvenliği iyileştirmelerini de içerecek şekilde, hazırlar.

MADDE 12 – (1) Denetimin, birim düzeyinde yapılması durumunda değerlendirme konuları, bilgi ve iletişim güvenliği sistemi ile sınırlıdır.

Bilgi ve İletişim Güvenliği Sistemi Oluşturma Çalışmaları Kapsamındaki Harcamalar

MADDE 13 – (1) Bu Yönerge kapsamında, üniversite tarafından gerçekleştirilecek çalışmalara ilişkin her türlü harcama, üniversitenin bütçesine ilgili konuda tahsis edilecek ödenekle karşılanır.

ALTINCI BÖLÜM
Çeşitli ve Son Hükümler

Hüküm Bulunmayan Haller

MADDE 14 - (1) Bu Yönerge'de hüküm bulunmaması halinde T.C. Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve ilgili mevzuat hükümleri uygulanır.

Yürürlük

MADDE 15 - (1) Bu Yönerge, Senatoda kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 16 - (1) Bu Yönerge hükümlerini Çanakkale Onsekiz Mart Üniversitesi Rektörü yürütür.

EK: Üniversite Bilgi ve İletişim Güvenliği Sistemi Organizasyon Yapısı