T.C.
ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI
Coğrafi Bilgi Sistemleri Genel Müdürlüğü

Sayı : 90743779/010.06/4476 30../12./2014
Konu : Bilgi Güvenliği Politikaları

GENELGE

(2014/27)

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

MADDE 1 - (1) T.C. Çevre ve Şehircilik Bakanlığı olarak, iş sürekliliğimizi sağlamak, bilgi varlıklarımıza yönelik kasıtlı veya kasıtsız her türlü tehdidi tanımlamak ve riskleri yönetmek amacıyla;

a) ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardına uygun bir yönetim sistemi kurmak, işletmek ve sürekli iyileştirmek.

b) Kurumsal bilgilerin gizliliğini, doğruluğunu ve bütünlüğünü korumak,

c)Halka hizmet verilen tüm çevrimiçi sistemlerin sürekli olarak erişilebilirliğini sağlamak,

ç) Personeli bilgi güvenliği anlamında bilinçlendirmek amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimleri gerçekleştirmek,

d) Bilgi teknolojileri alanında meydana gelen gelişim ve değişime uyum sağlamak amacıyla dinamik bir yapı oluşturmak ve otoriteler ile iletişimleri artırmak,

e) Bilgi Güvenliği alanında en büyük kapsamda sertifikalandırmayı gerçekleştirmektir.

Kapsam

MADDE 2 - (1) Bu Genelge kapsamında belirtilen esaslar Bakanlık Merkez Teşkilatında bulunan bütün birimlerdeki personelin, bilgi sistemine yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsar.

Dayanak

MADDE 3 - (1) Bu Genelge kapsamında belirtilen hususlar 4.7.2011 tarih 27984 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Çevre ve Şehircilik Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 13. Maddesinin birinci fıkrasının (i) bendi, 23.05.2007 tarih ve 26530 sayılı Resmi Gazetede yayınlanan 5651 sayılı Kanunun 6. Maddesi ve ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı uyarınca hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Genelgenin uygulanmasında;

a) Bakan: Çevre ve Şehircilik Bakanını,

Söğütözü Mah. 2179 Sok. No:5 Balgat/Ankara İrtibat: Mevzuat Şube Müdür V. Hayal TERECİ ÇELİK
Tel: 0 312 285 71 73/2098 Fax:0312 286 2614 E Posta: hayal.tereci@csb.gov.tr

b) Bakanlık: Çevre ve Şehircilik Bakanlığını,

c) BGYS: Bilgi Güvenliği Yönetim Sistemi,

ç) Bilgi: Kurum için değeri olan, uygun bir şekilde korunması gereken tüm kaynakları,

d) Bilgi güvenliği: Bilgi ve bilginin işlem gördüğü bilgi sistemlerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümünü,

e) Bilgi Sistemleri: Donanım, yazılım, veri, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü,

f) Genel Müdürlük: Coğrafi Bilgi Sistemleri Genel Müdürlüğü'nü,

g) Kılavuz: Bilgi Güvenliği Politikaları Klavuzunu,

ğ) TS ISO/IEC 27001: Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements) Standartı,

h) Veri: Bilginin işlenmemiş halini,

ı) Yönetici: Bilgi Güvenliği Yönetim Sistemi Yöneticileri,

i) Yönetim Sistemi Performans Raporu: BGYS Yöneticileri ve BGYS Sorumluları tarafından BGYS'nin performansının izlenerek belirli aralıklarda oluşturulan raporu ifade eder.

İKİNCİ BÖLÜM
Bilgi Güvenliği Politikaları

Bilgi sistemleri genel kullanım politikası

MADDE 5 - (1) Bilgi Güvenliği Politikası ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Kurum personeli ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

(2) Bu kural ve prosedürler, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

(3) Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001:2013 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.

(4) BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların da katkısıyla, Coğrafi Bilgi Sistemleri Genel Müdürlüğü, Bilgi İşlem Dairesi Başkanlığı yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yöneticisi sorumluluğundadır. Ek, form, talimat gibi dokümanların güncellenmesi ise ilgili daire başkanlığı/şube müdürlüklerinin sorumluluğundadır.

(5) Kurum tarafından personele veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça kuruma aittir.

(6) Personelin bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak kurum personeline ve yeni işe giren personele verilir.

(7) Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir, ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar etmesini engelleyici önlemler alınır.

ÜÇÜNCÜ BÖLÜM
Bilgi Güvenliği Organizasyonu

BGYS üst yöneticisi

MADDE 6 – (1) Bakanlık merkez teşkilatı bünyesinde bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere Coğrafi Bilgi Sistemleri Genel Müdürü, Genel Müdür Yardımcısı, Bilgi İşlem Daire Başkanı ve İlgili Şube Müdüründen oluşmaktadır. Görevleri;

a) BGYS kapsamındaki üst düzey dokümanları onaylatmak,

b) Kurumun stratejik planlarına uygun Bilgi Güvenliği Politikasını ve BGYS amaçlarını belirlemek,

c) BGYS'nin amaçlarına ulaşmak için gerekli olan tüm kaynakların ve sorumlulukların tahsislerini gerçekleştirmek, yatırım kararları almak,

ç) BGYS dokümanlarını onaylamak,

d) BGYS kapsamında ortaya çıkan artık riskleri onaylamak,

e) BGYS Yürütme ve Yönetim Komitesi toplantılarını organize etmek katılmak,

f) Kendisine yönlendirilen karar taleplerini karara bağlamaktır.

BGYS yürütme ve yönetim komitesi

MADDE 7 – (1) BGYS üst yöneticileri ve BGYS yöneticilerinden oluşmakta olup, çalışma usul ve esasları ile görevleri aşağıdaki gibidir;

a) Yılda en az bir kez ve ihtiyaç durumlarında toplanır.

b) Komiteye üst yönetici veya yerine belirleyeceği birisi başkanlık eder.

c) BGYS Komitesi tarafından iletilen raporları, risk ve fırsatları, sorunları değerlendirir ve karar verir.

ç) Kapsam, organizasyon yapısı, politika gibi üst seviye dokümanları gözden geçirir, değişikliklerini değerlendirir ve karar verir.

d) Yatırım ihtiyaçlarını değerlendirir ve karar verir.

BGYS komitesi

MADDE 8 – (1) BGYS Yöneticileri ve kapsam dâhilindeki birimlerin BGYS sorumlularının katılımıyla kurulan komitedir. Çalışma usul ve esasları ile görevleri aşağıdaki gibidir;

a) BGYS'nin işletilmesi ve sürdürülmesi için gerekli çalışmaları yapmak amacı ile altı ayda en az bir kez ve ihtiyaç durumlarında toplanır.

b) BGYS'nin temelini oluşturan varlık envanteri ve risk analizi çalışmalarını gözden geçirir.

Söğütözü Mah. 2179 Sok. No:5 Balgat/Ankara İrtibat: Mevzuat Şube Müdür V. Hayal TERECİ ÇELİK
Tel: 0 312 285 71 73/2098 Fax:0312 286 2614 E Posta: hayal.tereci@csb.gov.tr

c) Seçilmiş olan risk müdahale yöntemi ve kontrollerin uygunluğunu değerlendirir.

ç) BGYS operasyon ve uygulamalarının ISO 27001 standardına uygunluğunu kontrol eder.

d) BGYS'nin değişen iş ve yasal gereksinimlere uyumunu sağlar.

e) İş sürekliliği tatbikat sonuçlarını ve güvenlik ihlal olaylarını değerlendirir.

f) BGYS Yürütme ve Yönetim Komitesi' ne raporlama yapar.

BGYS yöneticisi

MADDE 9 – (1) Bakanlık merkez teşkilatı bünyesinde bilgi güvenliği faaliyetlerini yürütülmesi için gerekli alt yapıyı hazırlamak üzere Bilgi İşlem Dairesi Başkanlığınca görevlendirilmiş personelden oluşur, görevleri;

a) BGYS'nin kurulması ve işletilmesini sağlamak.

b) BGYS'nin performansını izlemek ve sonuçlarını BGYS Üst Yöneticisi'ne belirlenen periyotlarda raporlamak (Yönetim Sistemi Performans Raporu).

c) Yönetim Gözden Geçirme toplantılarını koordine etmek

ç) BGYS İç Tetkiklerini koordine etmek ve sonuçlarını değerlendirmek

d) BGYS dokümanlarını oluşturmak veya oluşturulmasını sağlamak

e) BGYS dokümanlarının kontrolünü ve güncellemesini yapmak

f) BGYS dokümanlarının güncel hallerinin BGYS yazılımında erişilebilir olmasını sağlamak

g) Çalışanların bilgi güvenliği farkındalık eğitimlerini koordine etmek ve eğitimlerin etkinliklerini değerlendirmek

ğ) BGYS Yöneticileri ve Sorumlularının bilgi güvenliğine ilişkin olarak karşılaşabileceği riskleri anlaması ve tanıması için gerekli eğitici yöntemleri koordine etmek

h) Risk analizi sonuçlarını değerlendirmek, kontrollerin belirlenmesi ve uygulanmasını koordine etmek

ı) Bilgi Güvenliği ihlal olaylarını değerlendirmek ve takibini yapmak

i) Bilgi Güvenliği'ne ilişkin Düzenleyici Faaliyetleri takip etmek ve kayıtları onaylamak

j) Bilgi Güvenliği Politikası'nı belli aralıklarla gözden geçirmek ve BGYS Üst Yöneticisi'ne bildirerek Üst Yönetim tarafından onaylamasını sağlamak

k) Kapsam dahilinde gerçekleştirilen tüm projelerin bilgi güvenliği açısından değerlendirilmesini sağlamak

l) BGYS Yürütme ve Yönetim Komitesi toplantılarını koordine etmek ve katılmak

m) BGYS Komitesi toplantılarını koordine etmek ve katılmak

n) Mevcut güvenlik cihazlarını yönetmek ve Log(İz Kaydı) yönetimini yapmak

BGYS sorumluları

MADDE 10 – (1) Bakanlık merkez teşkilatı bünyesindeki başkanlıklardan seçilen kendi birimindeki bilgi güvenliği faaliyetlerini yürütmesi amacıyla üst yönetim tarafından görevlendirilmiş personel olup, görevleri;

Söğütözü Mah. 2179 Sok. No:5 Balgat/Ankara İrtibat: Mevzuat Şube Müdür V. Hayal TERECİ ÇELİK
Tel: 0 312 285 71 73/2098 Fax:0312 286 2614 E Posta: hayal.tereci@csb.gov.tr

a) BGYS'nin kurulmasına ve işletilmesinde BGYS Yöneticisi'ne destek olmak

b) Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nde süreçlerin bilgi güvenliği gereksinimlerine uygun bir şekilde gerçekleştirildiğini kontrol etmek

c)Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'ne ait varlık envanterinin güncelliğini sağlamak, yeni bir varlık eklendiği zaman "Güvenlik İhtiyaç Listesi" ni doldurarak BGYS Yöneticisine iletmek,

ç) Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nün BGYS kapsamındaki riskler ile ilgili bildirimleri ve takibini yapmak,

d) Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nün Yönetim Sistemi Performans Raporu belirlenen sıklıklarda hazırlamak ve BGYS Yöneticisine sunmak,

e) Bilgi Güvenliği Politikasının kapsamını, politika çerçevesindeki yetki ve sorumlulukları, aday memur eğitim programı dahilinde işe yeni başlayan personele duyurmak

f) Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nde tespit ettikleri bilgi güvenliği ihlal olaylarını "Bilgi Güvenliği İhlal Olayları Yönetimi Prosedürü"ne uygun olarak raporlamak,

g) Hizmet alınan 3.tarafların ilgili BGYS Politika ve prosedürlerine uygun şekilde çalıştığını denetlemek,

ğ) BGYS Yöneticisinin koordinesinde gerçekleşecek olan planlı iç tetkiklerde bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nü koordine etmek, BGYS yöneticisine yardımcı olmak,

h) Daire Başkanlığı/Şube Müdürlüğü'nde başlatılan veya aksiyon alınması kendilerine atanan düzeltici ve iyileştirici faaliyetlerin takibini yapmak, sonuçlarını bildirmek,

ı) BGYS dokümanlarının hazırlanmasına, güncellenmesine katkı sağlamak ve doküman hazırlamak,

i) Bağlı bulunduğu Daire Başkanlığı/Şube Müdürlüğü'nde gerçekleşen tüm projelerin bilgi güvenliği açısından değerlendirilmesi için "Proje Yönetimi Bilgi Güvenliği Formu" nu doldurarak BGYS Yöneticisi ile iletişime geçmek,

j) BGYS sorumluları yaptıkları iş ve işlemlerden Birim Yöneticilerine karşı sorumlu olup, Birim Yöneticilerin Sorumlulukları "Roller ve Sorumluluklar Yeterlilik İletişim Klavuzu"nda tanımlanmıştır.

DÖRDÜNCÜ BÖLÜM
Bilgi Güvenliği İhlal Yönetimi

Bilgi güvenliği ihlal yönetimi

MADDE 11 - (1) Bilgi güvenliği olaylarının tespit edilmesi; Kurum çalışanları şüpheli buldukları durumlarda acil bir şekilde kurumsal yardım masası üzerinden olay bildirimi yaparak iletişime geçerler. BGYS Yöneticisi gelen olay bildirimlerini veya kurum güvenlik yazılımları aracılığıyla belirlenen bilgi güvenliği ihlal olaylarındaki şüpheli durumları tespit etmek ve yönetmekle sorumludur.

(2) Bilgi güvenliği olaylarının raporlanması ve değerlendirilmesi; Bilgi güvenliği ihlal olayı tespiti sonrası olayla ilgili deliller toplanacak ve müdahale için sınıflandırılacaktır. Tüm çalışanlar ve 3. Taraflar için raporlama mekanizması mümkün olduğunca, kolay erişilebilir ve kullanılabilir olmalıdır. Raporlama müdahale için gerekli

bilgileri kapsayacak detayda olmalı ve kayıtlar içermelidir. Olayların önceliklendirilmesi için olayın etkisini, kapsamını ve sınıflandırılmasını belirlemek amacıyla BGYS yöneticileri verileri inceleyecektir.

(3) Bilgi güvenliği olaylarına müdahale edilmesi; Kontroller veya bildirilen durumlar ile tespit edilen ve delilleri toplanan tüm olaylar için diğer işlemlerden önce olaya sebep olan açıklık kapatılmalıdır. Açıklıkların kapatılmasından sonra mutlaka kontroller tekrarlanmalı ve açıklığın kapandığı onaylanmalıdır.

(4) Bilgi güvenliği önlem alınması ve deneyim edinilmesi; Tespit edilen, delilleri toplanan ve daha sonra oluşmasına sebep olan açıklıkların kapatılması sonrasında mutlaka her bir olay için tekrar oluşmasını engellemek için önlemler alınmalıdır.

(5) Bilgi güvenliği kayıt ve kanıt toplanması; Olayın tespiti ve sorumlunun belirleneceği kayıtların bütünlüğünün bozulmadığı kontrol edilmelidir. Bütünlüğü kanıtlanamayan kayıtlar için işlemler yapılmamalıdır.

BEŞİNCİ BÖLÜM
Bilgi Güvenliği Politikaları Kılavuzu ve Uygulanması

Bilgi güvenliği politikaları kılavuzu

MADDE 12 - (1) Kılavuz, Genel Müdürlük tarafından kapsam maddesinde tanımlanan tüm unsurlarla ilgili olarak; bilgi güvenliğinin sağlanması ile ilgili; yönetsel, teknik, idari, hukuki süreçlerin tüm detaylarının yer alacağı bir doküman olarak hazırlanır.

(2) Kılavuzun ilk versiyonu Bakanın onayı ile yürürlüğe girer, daha sonraki versiyonlar Müşteşarlık onayı ile yürürlüğe konulur.

(3) Kılavuz; periyodik olarak, teknolojik gelişmeler paralelinde gözden geçirilerek revize edilir ve elektronik ortamda yayınlanacak bir rehber doküman olarak hazırlanır.

(4) Kapsam maddesinde belirtilen tüm Bakanlık Merkez Teşkilatı, kılavuzda yer alan hususlara uymakla yükümlüdür. Gerekli hallerde Genel Müdürlükçe teknik destek talepleri karşılanır. Genel Müdürlük, Bakanlık internet ana sayfası üzerinde bilgi güvenliği bağlantı adresi oluşturur. Bu bağlantı adresi üzerinden açılan internet sayfasında bilgi güvenliği konularında üretilen ulusal ve uluslararası kılavuz, rapor, bilgi notu, tez vb. dokümanlarına erişim sağlanır.

(5) Genel Müdürlük, Bilgi Güvenliği Terimleri Sözlüğü hazırlar ve internet üzerinden yayına sunar.

Kılavuzun uygulanması

MADDE 13 - (1) Kılavuzun uygulanması ile ilgili olarak; yöneticiler hazırlayacakları bilgi güvenliği planları içerisinde "Kılavuza Uyumlaşma Takvimi " hazırlar ve kılavuzun uygulanması ile ilgili gerekli idari tedbirleri alır.

ALTINCI BÖLÜM
Bilgi Güvenliği Eğitimleri ve Standartları

Bilgi güvenliği eğitimleri

MADDE 14 - (1) Genel Müdürlük, bilgi güvenliği eğitim planlamasını tüm Bakanlık merkez

Söğütözü Mah. 2179 Sok. No:5 Balgat/Ankara İrtibat: Mevzuat Şube Müdür V. Hayal TERECİ ÇELİK
Tel: 0 312 285 71 73/2098 Fax:0312 286 2614 E Posta: hayal.tereci@csb.gov.tr

teşkilatı için yapmak suretiyle her seviyedeki personelin bilgi güvenliği farkındalık düzeylerini artırmak yönünde eğitim faaliyetlerinde bulunur. Yıllık hizmet içi eğitim planlamalarında bilgi güvenliği başlığı planlara dahil edilir. Teknik seviyedeki personelin bilgi düzeyinin artırılması yönünde ileri seviyede bilgi güvenliği eğitim planlamalarını yapar.

(2) Ulusal düzeyde siber güvenlik ile ilgili kurum ve kuruluşlarla ortak eğitim, seminer, konferans, sempozyum gibi faaliyetler gerçekleştirilmesine yönelik yıllık planlar yapar.

(3) Bilgi güvenliği ile ilgili teknik ve farkındalık eğitimler BGYS portalı üzerinden web tabanlı olarak sunar.

Bilgi güvenliği standartları

MADDE 15 - (1) Genel Müdürlük bilgi güvenliği çalışmalarının standartlaştırılması ve çalışmalara sistematik bir anlayış entegre edilmesi yaklaşımı ile ulusal ve uluslararası bilgi güvenliği standartlarına uyumlaşmanın ve sertifikasyonun gerçekleştirilmesi yönünde çalışmalar yapar. Bu konuda ulusal ve uluslararası kuruluşlarla işbirliği gerçekleştirir.

YEDİNCİ BÖLÜM
Son Hükümler

Uygulama

MADDE 16 - (1) Bu Genelge kapsamında yürütülecek iş ve işlemlerde Genelge ekinde yer alan, Çevre ve Şehircilik Bakanlığı "Bilgi Güvenliği Politikaları Klavuzu" esas alınır.

Yürürlük

MADDE 17 - (1) Bu Genelge, Çevre ve Şehircilik Bakanının onayı ile yürürlüğe girer.

Yürütme

MADDE 18 - (1) Bu Genelge hükümlerini Çevre ve Şehircilik Bakanı yürütür.

İdris GÜLLÜCE
Bakan

DAĞITIM:
Bilgi ve Gereği:
-Merkez Teşkilatı

Söğütözü Mah. 2179 Sok. No:5 Balgat/Ankara İrtibat: Mevzuat Şube Müdür V. Hayal TERECİ ÇELİK
Tel: 0 312 285 71 73/2098 Fax:0312 286 2614 E Posta: hayal.tereci@csb.gov.tr