TÜRKİYE CUMHURİYETİ
CUMHURBAŞKANLIĞI
SİBER GÜVENLİK
BAŞKANLIĞI

SIKÇA SORULAN SORULAR

BİLGİ ve İLETİŞİM GÜVENLİĞİ FAALİYETLERİ

TEMMUZ 2026

BELGE ADI: Bilgi ve İletişim Güvenliği Faaliyetleri Sıkça Sorulan Sorular

SÜRÜM NO: 1.1

SÜRÜM TARİHİ: 02.07.2026

GİZLİLİK DERECESİ: Tasnif Dışı

Değişiklik No	Değişiklik Tarihi	Değişiklik Nedeni
1.0	Mayıs 2026	İlk Yayın
1.1	Temmuz 2026	Kapak Değişikliği İçerik Güncellenmesi

İçindekiler Tablosu

1. Bilgi ve İletişim Güvenliği Genelgesi

Genelgenin amacı nedir?

İçinde bulunduğumuz çağın en kıymetli unsurlarından biri olan veriyi, hem korumak hem de işleyip değere dönüştürmek ülkemizin öncelikli meseleleri arasındadır. Veri güvenliğine yönelik son dönemde yaşanan hadiseler, ülkelerin sınırları kadar verilerini ve dijital altyapılarını da korumasının önemini göstermiştir. Siber güvenlik ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Bu kapsamda, ülkemizin verisinin ülkemizde kalması, kurumların, şirketlerin ve hatta bireylerin veri mahremiyeti konusunda riskli yaklaşımlara karşı bilinçli olması, yerli ve milli çözümler geliştirilmesi ve kullanılması, karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amaçlanmış ve uygulamada görülen aksaklıklara yönelik genel prensip mahiyetinde bazı tedbirlerin alınması uygun görülmüştür.

Genelge hangi kurumları kapsamaktadır?

Genelge, tüm kamu kurum ve kuruluşları ile kritik altyapı sektörlerinden **"Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Ulaştırma", "Bankacılık ve Finans"** sektörleri ile nüfus, sağlık, güvenlik gibi alanlarda "Kritik Kamu Hizmetleri" sunan işletmeleri kapsamaktadır. Kritik altyapı işleten özel hukuk tüzel kişiler hariç olmak üzere, diğer özel hukuk tüzel kişileri kapsamamakla beraber genelgede yer alan tedbirlerin uygulanması bu kurumların yararına olacaktır.

Genelgenin yürürlük tarihi nedir?

Genelgenin yürürlük tarihi Resmî Gazetede yayınlandığı tarih olan 06.07.2019 dur. Genelgede yer verildiği üzere, mevcut bilgi teknolojisi altyapılarının, belirtilen tedbirlere uyumlu hale getirilmesi, yayımlanmasını müteakip rehberde yer alacak plan çerçevesinde, güvenlik seviyesi öncelikleri dikkate alınarak ve kademeli olarak sağlanacaktır.

Genelge kapsamında denetimleri kim yapacaktır, yaptırımlar neler olacaktır?

Genelgede ve yayımlanan Rehberde yer alan güvenlik tedbirlerinin uygulanmasına ilişkin denetimler, en az yılda bir kere olmak üzere, kurum ve kuruluşların iç denetim mekanizmaları yoluyla yapılır. Genelge ve Rehberde yer alan tedbirlerin uygulanmasına yönelik yapılacak denetimler bilgi güvenliğini sağlamaya yönelik olmakla birlikte, söz konusu tedbirlere uyulmaması nedeniyle bir zafiyet oluşması durumunda halihazırda ilgili mevzuatta belirlenen yaptırımlar geçerlidir. Oluşabilecek zararın boyutuna göre gerek duyulması durumunda kurum içi adli veya idari soruşturma süreçleri işletilebilecektir.

Gizli veri, kritik veri, kritik kurum gibi ifadelerin tanımı nedir?

Genelgede yer alan terimlere ait tanımlamalara Bilgi ve İletişim Güvenliği Rehberinde yer verilmiştir.

"Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli ağda tutulacak" ifadesi ile anlatılmak istenen nedir?

Ağ, sistem ve veri güvenliği kapsamında, internetten sunulma zorunluluğu bulunmayan ve rehberde yer alacak "kritik veri" tanımı kapsamına giren verilerin internet ağından yalıtılmış, fiziksel güvenlik tedbirleri alınmış, erişim yetkileri sınırlandırılmış bir ağda bulundurulması amacıyla alınmış bir tedbirdir.

Genelge ile Bulut hizmetleri yasaklanmakta mıdır? "Kurum kontrolündeki yerli hizmet sağlayıcılar" cümlesinde belirtilen "kurum kontrolü" ifadesi ne anlama gelmektedir?

Genelgenin ilgili maddesi bulut teknolojisinin kullanımına dair bir çerçeve çizmekte, ülke verisinin ülkede kalmasını hedeflemektedir. Bulut hizmeti alınırken verilerin ülke içindeki veri merkezlerinde depolanması ve güvenlik kontrollerinin sağlanması kaydıyla yerli veya yabancı bulut servislerinden yer, sunucu veya hizmet kullanımına yönelik bir yasaklama getirmemektedir. "Kurum kontrolü", bulut hizmeti veren sistemlere erişen personel ve yetki düzeyleri, sunucuların kuruma tahsisli olup olmadığı, erişim ve işlem loglarının izlenebilmesi gibi veri güvenliğine yönelik kontrolleri ifade etmektedir.

Üretici ve tedarikçilerden taahhütname alınması ile ilgili nasıl bir yol izlenmektedir?

Genelgenin ilgili maddesi, bazı ülkelerin, üreticilerine istihbarat amaçlı arka kapı bırakma zorunluluğu getirme girişimleri de göz önünde bulundurularak, uygulama, veri ve sistem güvenliği kapsamında, yazılım ve donanımlarda kasıtlı oluşturulan arka kapı zafiyetlerine karşı alınan bir tedbirdir. Kurum ve kuruluşlarca yapılacak yazılım ve donanım teminleri için hazırlanacak şartnamelerde bu konuda hassasiyet gösterilmesi, mümkünse ürünün arka kapı içermediğine dair taahhütname alınması istenmektedir. Taahhütname alınsın veya alınmasın, arka kapı tespiti durumunda, mevcut mevzuat çerçevesinde adli ve idari soruşturma süreçlerinin işletilmesi, arka kapı zafiyetinin duyurularak alımın iptali ve firmanın yasaklı duruma düşürülmesi gibi yaptırımlar uygulanabilecektir.

Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile personeli hakkında güvenlik soruşturması veya arşiv araştırması yapılması ile ilgili madde kapsamında, mevcut çalışanlara tekrar güvenlik soruşturması yapılması gerekecek mi?

Söz konusu madde kapsamına giren görevleri nedeniyle halihazırda hakkında güvenlik soruşturması veya arşiv araştırması yapılmış bulunan ilgili üst yönetici veya personel için gerekli görülmedikçe güvenlik soruşturması ve arşiv araştırmasının yenilenmesine ihtiyaç bulunmamaktadır. Ancak ilgili yönetmelik çerçevesinde, gerekli görülen hallerde güvenlik soruşturması ve arşiv araştırmasının yenilenmesi mümkündür.

21.Maddede belirtilen tedbirin kapsamı nedir?

Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurum ve kuruluşlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, doğrudan bu kurumlara haberleşme hizmeti sağlayan baz istasyonlarının ve diğer haberleşme sistemlerinin transmisyon altyapısında ilk toplama noktasına kadar radyolink bağlantısı kullanılmaması, kullanımın zorunlu olduğu durumlarda milli kripto sistemleriyle kriptolanarak kullanılması söz konusu maddenin kapsamını oluşturmaktadır.

İnternet değişim noktasını kimler kurmak zorundadır?

Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmecilerce yerine getirilmek üzere, veri güvenliği, iletişim güvenliği ve yurt içi iletişim trafiğinin yurt dışına çıkarılmamasına yönelik genel çerçeveyi belirten düzenleyici bir tedbirdir. Söz konusu tedbirin uygulanmasına ilişkin teknik, hukuki ve ticari hususlar yetkili düzenleyici ve denetleyici kurum tarafından yapılacak düzenlemeyle belirlenecektir.

2. Bilgi ve İletişim Güvenliği Rehberi

Bilgi ve İletişim Güvenliği Rehberi'nin mevzuat dayanağı nedir?

06.07.2019 tarih ve 30823 sayılı Resmî Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Mezkûr Genelge'de "*Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve www.cbddo.gov.tr adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir.*" ibaresi yer almakta ve Bilgi ve İletişim Güvenliği Rehberi'ne dayanak teşkil etmektedir.

177 nolu Cumhurbaşkanlığı Kararnamesi ile Siber Güvenlik Başkanlığı kurulmuş, Dijital Dönüşüm Ofisi'nin siber güvenlik alanındaki görevleri Siber Güvenlik Başkanlığına aktarılmıştır. Akabinde yayımlanan 7545 sayılı Siber Güvenlik Kanunu ile Başkanlığın yetkileri düzenlenmiş, Dijital Dönüşüm Ofisi'nin siber güvenlik alanındaki her türlü uygulaması ve envanteri Başkanlığa devredilmiştir.

Bilgi ve İletişim Güvenliği Rehberi'nin kapsamında hangi kurum ve kuruluşlar yer almaktadır?

Bilgi ve İletişim Güvenliği Rehberi, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmelerden bilgi işlem birimi barındıranları veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alanları kapsamaktadır.

Bilgi ve İletişim Güvenliği Rehberi'nde bahsi geçen kritik altyapı sektörleri hangileridir?

Rehberde bahsi geçen kritik altyapı sektörleri "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma", "Bankacılık ve Finans"dır.

5 Mayıs 2026'da yapılan ilk Siber Güvenlik Kurulu toplantısında "Dijital Altyapılar, Dijital Hizmetler, Elektronik Haberleşme, Enerji, Finans, Gıda ve Tarım, İmalat Sanayi, Kamu Hizmetleri, Medya ve Kriz İletişimi, Posta ve Kargo, Sağlık, Savunma Sanayii, Su Yönetimi, Ulaştırma, Uzay" alanlarının Kritik Altyapı Sektörleri olarak belirlenmesi kararlaştırılmıştır.

7545 Sayılı Siber Güvenlik Kanunu çerçevesinde kritik altyapı sektörlerini kapsayacak ikincil düzenlemelere ilişkin çalışmalar devam etmektedir.

Bilgi Güvenliği Yönetim Sistemi ile Bilgi ve İletişim Güvenliği Rehberi arasındaki etkileşim nasıl olmalıdır?

Kurumlar hâlihazırda yürüttükleri bilgi güvenliği yönetim sistemi (BGYS) süreçlerini varlık – kontrol veya süreç – kontrol temelli bir yaklaşımla ele almaktadır. BGYS'de yer alan varlık veya süreçlerin bilgi güvenliğine mevcut etkisi ve bilgi güvenliği kapsamında belirlenen risklerin gerçekleşme olasılığı tanımlanarak risk analizi faaliyeti gerçekleştirilir. Risk analizi sonucunda kurum, kuruluş ve işletmeler kabul edebileceği risk değerini belirleyerek, bu değerin üzerinde kalan risklere yönelik düzeltici, önleyici ve iyileştirici faaliyetler gerçekleştirir.

Bilgi ve İletişim Güvenliği Rehberi'nde, varlık grupları oluşturularak bunların bilgi güvenliğine olan etkisini belirlemek üzere anket çalışması yapılır. Anket çalışmasında Delfi metodu kullanılır. Anket çalışması sonucunda ortaya çıkan puan varlık grubunun kritiklik derecesini belirler. Belirlenen kritiklik derecesine karşılık gelen tedbirler varlık grubuna uygulanır. Dolayısıyla BGYS'de varlık özelinde yapılan çalışmalar, Rehber'de varlık grupları üzerinden yapılmaktadır.

Rehber, BGYS'deki risk analiz faaliyetleri sonrasında uygulanacak kontrollere, her varlık grubu ve kritiklik derecesi özelinde tedbirler sunarak daha güvenilir ve ayakları yere basan bir bilgi güvenliği yönetim sistemi kurulmasını sağlar. Bunlarla birlikte Rehber'de yer alan denetim soruları BGYS kapsamında gerçekleştirilecek iç tetkik faaliyetlerini destekleyerek kurum, kuruluş ve işletmeler için daha güvenilir bir iç kontrol ortamı oluşturulmasına zemin hazırlar.

Varlık grubu kritiklik derecesi nasıl belirlenir?

Rehber'de yer alan varlık grupları altı temel başlık altında tanımlanmıştır ve ilgili başlıklar aşağıda yer almaktadır.

1. Ağ ve Sistemler
2. Uygulamalar
3. Taşınabilir Cihaz ve Ortamlar
4. IoT Cihazları
5. Personel
6. Fiziksel Mekânlar

Varlıkların kritiklik derecesini belirlemek için öncelikli olarak varlık grupları Rehber'in 22. sayfasında yer alan hususlara uygun olarak tanımlanmalıdır. Her bir varlık grubu başlığı özelinde birden çok varlık grubu tanımlanabilmektedir.

Örneğin; Uygulamalar varlık grubu çerçevesinde Uygulamalar 1, Uygulamalar 2, … , Uygulamalar N gibi birden fazla varlık grubu tanımlanabilmekte ve Uygulamalar 1, Uygulamalar 2, … , Uygulamalar N varlık grubu içeresinde ise birden çok uygulama varlık olarak tanımlanabilmektedir.

Bir başka deyişle; Uygulamalar 1 varlık grubuna kurumun dışarıya açık olan uygulamaları (Web Tabanlı Uygulama 1, Web Tabanlı Uygulama 2, … , Web Tabanlı Uygulama N) tanımlanabilirken, Uygulamalar 2 varlık grubuna kurumun dışarıya açık olmayan uygulamaları (Web Tabanlı Uygulama 1, Masaüstü Uygulaması 1, … ,Web Tabanlı Uygulama N) tanımlanabilir.

Bu şekilde bir tanımlamada Uygulamalar 1 in varlık grubu kritiklik derecesi belirlenirken anket soruları bu grup içerisinde tanımlı olan en kritik ve en etkili varlık dikkate alınarak yanıtlanmalıdır. Anket çalışmasına varlıkların sahipleri, sistem yöneticileri, geliştiriciler, kullanıcı temsilcileri, yöneticileri ve kurumun sahip olduğu en yetkin personel katılım sağlamalıdır. Aynı süreç Uygulamalar 2 içinde benzer şekilde yürütülmelidir.

Bilgi ve İletişim Güvenliği Rehberi çerçevesinde mevcut durum ve boşluk analizi nasıl yapılır?

Varlık grupları ve kritiklik dereceleri belirlendikten sonra Rehber'in Varlık Gruplarına Yönelik Güvenlik Tedbirleri'nden (3. Bölüm) varlık grubuna ve kritiklik derecesine uygun tedbirler belirlenir, daha sonra Uygulama ve Teknoloji Alanına Yönelik Güvenlik Tedbirleri (4. Bölüm)

ile Sıkılaştırma Tedbirleri'nden (5. Bölüm) varlık grubu ile ilgili olan alt başlıklar ve bu alt başlıklardan varlık grubunun kritiklik derecesine uygun olan tedbirler belirlenir.

Mevcut durum analizi; varlık grupları için belirlenen tüm tedbirlerin mevcut durumda uygulanıp uygulanmadığı, uygulanıyor ise varlık grubunda yer alan varlıkların tamamına, çoğuna ya da bir kısmına uygulandığının tespit edilmesi ve Mevcut Durum Analizi ve Boşluk Analizi Formu'na (EK - C.3) işlenmesi ile gerçekleştirilir.

Varlık grubuna uygulanmak üzere belirlenen tedbirlerden; uygulanmayan veya kısmen uygulananlar listelenerek boşluk analizi çalışması gerçekleştirilir. Hedeflenen duruma erişmek için yapılması gereken çalışmalar Mevcut Durum Analizi ve Boşluk Analizi Formu'na (EK-C.3) işlenir.

Mevcut durum analizi çalışmaları kapsamında teknik çalışma, toplantı, otomatik araç ile durum tespiti, dokümantasyon inceleme vb. faaliyetlerden yararlanılabilir.

Bilgi ve İletişim Güvenliği Rehberi çerçevesinde varlık gruplarının kritiklik derecesini belirleyen kriterler nelerdir?

Bilgi ve İletişim Güvenliği Rehberi'nde yer alan her bir varlık grubunun kritiklik derecesi; işlenen verinin gizlilik, bütünlük ve erişilebilirlik açısından kritikliği ile olası güvenlik ihlallerinin etki alanları yani varlık grubuna bağımlı varlıklar, etkilenen kişi sayısı, kurumsal sonuçlar, sektörel etki ve toplumsal sonuçlar dikkate alınarak oluşturulan (EK- C.1) anket sorularına göre belirlenmektedir.

Her bir varlık grubu için bu anket formu doldurularak ilgili varlık grubunun kritiklik derecesi belirlenir.

Rehber'de yer alan "Gizlilik Dereceli Bilgi/Veri" ile "Kritik Bilgi/Veri"nin farkı nedir?

Rehber kapsamında Gizlilik Dereceli Bilgi/Veri, "*Bilmesi gereken dışındakilere açıklanması veya verilmesi milli güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine "ÇOK GİZLİ", "GİZLİ", "ÖZEL" veya "HİZMETE ÖZEL"* şeklinde sınıflandırılan bilgi/veri." şeklinde tanımlanmıştır.

Burada yapılan sınıflandırmada bilgi ve verinin gizlilik derecesi temel kriterdir.

Rehberde Kritik Bilgi/Veri;

- *"Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri,*
- *Kritiklik derecesi 3 olarak hesaplanan varlıkların işlediği veriler,*
- *24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan özel nitelikli kişisel veriler." şeklinde tanımlanmıştır.*

Kritik bilgi ve verinin belirlenmesinde temel kriter gizlilik derecesi değildir. Kritik bilgi/verinin belirlenmesinde, işlenen verinin gizliliği, bütünlüğü ve erişilebilirliği ile etki alanı boyutu önemlidir. Etki alanı boyutunda bilgi/veri ile ilgili; bağımlı varlıklar, etkilenen kişi sayısı, kurumsal sonuçlar, sektörel etki ve toplumsal sonuçlar yer almaktadır.

Bilgi ve İletişim Güvenliği Rehberi kapsamında yer alan kurum, kuruluş ve işletmelere hizmet sağlayan üçüncü taraflar Rehber'e uyum sağlamakla yükümlü müdür?

Bilgi ve İletişim Güvenliği Rehberi kapsamında yer alan kurum, kuruluş ve işletmelere hizmet sağlayan üçüncü taraflar Rehber'e uyum sağlamakla doğrudan yükümlü değildir. Ancak, kapsam dâhilindekiler, Rehber'in gerekliliklerine hizmet ve ürünlerin temini ve işletiminde uymakla yükümlü olduğundan üçüncü taraflarda dolaylı olarak hizmet ve ürünlerinde bu gereksinimlere uyum sağlayacaktır.

Bilgi ve İletişim Güvenliği Rehberi ile kamu personelinin kullandığı anlık mesajlaşma uygulamalarına herhangi bir kısıtlama getirilmekte midir?

Bilgi ve İletişim Güvenliği Rehberi'nin Anlık Mesajlaşma Güvenliği başlığı altında yer alan 4.2.1.1 tedbir maddesinde "*Kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan mesajlaşma uygulamaları kullanılmalıdır. Kurumun kendine ait bir haberleşme uygulaması yoksa mesajlaşma amacıyla sunucuları yurt içinde bulunan yerli ve milli uygulamalar tercih edilmelidir.*" ibaresi yer almaktadır. Tedbir maddesi sadece gizlilik içeren kurumsal haberleşme ve belge paylaşımına yöneliktir. Kamu personelinin kişisel haberleşme özelinde kullandığı anlık mesajlaşma uygulamalarına yönelik herhangi bir düzenleme ve kısıtlama bulunmamaktadır.

Bilgi ve İletişim Güvenliği Rehberi ile ilgili görüş, öneri ve sorular nasıl iletebilir?

Bilgi ve İletişim Güvenliği Rehberi ile ilgili her türlü soru, görüş ve öneri bgrehber[@]siberguvenlik[.]gov[.]tr e-posta adresine iletebilir.

Bilgi ve İletişim Güvenliği Rehberi uygulama sürecinde sorumlu olan personel birden fazla pozisyonda görevlendirilebilir mi?

Bilgi ve İletişim Güvenliği Rehberi uygulama sürecinde görev alacak personele ilişkin roller, Rehber içeriğindeki Sorumluluk Atama Matrisi'nde yer almaktadır. Örneğin; Bilgi Sistemleri Yöneticisi rolüne mümkün olduğu ölçüde bilgi işlem biriminin yönetiminden sorumlu amirin atanması gerekmektedir. Ancak bilgi işlem biriminin amiri aynı zamanda Kurumsal SOME Yöneticisi rolüne de üstleniyor ise bu durumda görevler ayrılığı prensibi uygulanarak her iki role farklı personel atanması uygun olacaktır. Özetle, Bilgi ve İletişim Güvenliği Rehberi uyum sürecinde yer alacak personelin yeterliliği ve yetkinliği de göz önünde bulundurularak, insan kaynağı ile ilgili bir eksiklik olmadığı sürece personelin birden fazla rolde görevlendirilmemesi tercih edilmelidir.

Varlıkların gruplanması nasıl yapılmalıdır?

Bilgi ve İletişim Güvenliği Rehberi'nde altı temel varlık grubu bulunmaktadır. Bunlar:

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihazlar ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

Kurumlar öncelikle sahip olduğu bilgi varlıklarının yukarıda belirtilen varlık gruplarından hangisi ile ilgili olduğunu belirlemelidir. Varlık grubu ile ilgili olduğu düşünülen kurumsal varlıklar kendi içinde güvenlik gereksinimleri, teknolojik özellikleri, hangi kurumsal ihtiyaçlara hizmet ettiği gibi kriterler göz önünde bulundurularak sınıflandırılmalıdır. Dolayısıyla yapılan sınıflandırma sonucu bir varlık grubunun altında varlık grubu ile ilgili birden fazla alt varlık grubu oluşabilir. Ancak tedbirlerin uygulanması noktasında daha etkin bir yaklaşımın

sağlanması amacıyla varlık grubu ana başlığı altında yer alan varlık gruplarının sayılarının yönetilebilecek sayıda olması önemlidir.

Bir varlığın birden fazla varlık grubuna dâhil olması durumunda hangi kritiklik derecesi dikkate alınmalıdır?

Birden fazla varlık grubu ile ilgili olduğu düşünülen kurumsal varlıklar, kritiklik derecesi en yüksek olan varlık grubu üzerinden değerlendirilmeli ve dâhil edildiği tüm varlık grupları ile ilgili tedbir maddeleri varlık için ele alınmalıdır.

Rehberde Elektronik Haberleşme sektörü ve Enerji sektörü için ayrı bir bölüm var. Bu iki sektör sadece bu bölümde yer alan tedbirleri uygulamakla mı yükümlüdür?

Kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar Rehberde yer alan tüm tedbirleri uygulamakla yükümlü olmakla birlikte ilaveten uygulanmak üzere Rehberde sektör özelindeki güvenlik tedbirlerine de yer verilmiştir.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesinin 21. Maddesinde belirtilen "kritik kurum" ifadesi Rehberde nasıl tanımlanmıştır?

Genelge'nin 21'inci maddesindeki tedbire ilişkin uygulama detayı Rehber'de *"Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri"* başlığının 4.5.3.14 maddesinde; *"Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır."* ifadesi ile yer almaktadır.

Genelge'nin 21. maddesinde belirtilen *"kritik kurum"* ifadesi Rehber'de *"Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumları"* olarak tanımlanmış olup, bu tanıma uymayan kurum ve kuruluşlar 21. madde kapsamına girmemektedir.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi dayanağında hazırlanan Bilgi ve İletişim Güvenliği Rehberi uyum, denetim ve gözetim faaliyetlerinin yürütülmesinde değişiklik olacak mı?

T.C. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı (Başkanlık) 177 no.lu Cumhurbaşkanlığı Kararnamesi ile kurulmuş olup mülga Dijital Dönüşüm Ofisinin siber güvenlik alanındaki görevleri Başkanlığa aktarılmıştır. Mezkûr kararnameyi takiben yayımlanan 7545 sayılı Siber Güvenlik Kanunu (7545 sayılı Kanun) ile Başkanlığın yetkileri düzenlenmiş, bu doğrultuda mülga Dijital Dönüşüm Ofisinin siber güvenlik alanındaki her türlü uygulaması ve envanteri Başkanlığa aktarılmıştır. Bu kapsamda Bilgi ve İletişim Güvenliği Rehberi uyum, denetim ve gözetim çalışmaları hâlihazırda Başkanlık bünyesinde sürdürülmektedir.

Kanun'un 5'inci maddesinin birinci fıkrasının (b), (ç), (h) bentleri uyarınca kamu kurumları ve kritik altyapıların siber dayanıklılığının artırılması ve bu hususta gerekli tedbirlerin alınması veya aldırılması, denetimlerin gerçekleştirilmesi ve sonucuna göre yaptırım uygulanması görevleri Başkanlığa tevdi edilmiştir. Başkanlık; Kanun'un 8'inci maddesi uyarınca Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilere ilişkin denetim faaliyetlerini program dâhilinde ve/veya program dışı gerçekleştirebilecektir.

Bununla birlikte Kanun çerçevesinde siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kritik altyapı sektörleri, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlara yönelik ikincil düzenlemelere ilişkin çalışmalar devam etmektedir.

Bilgi ve İletişim Güvenliği Rehberi güncellendi mi, teknik olarak ne değişti?
Siber Güvenlik Başkanlığın kurumsal kimliğinin yansıtılması amacıyla Bilgi ve İletişim Güvenliği Rehberi ile Denetim Rehberi'nde logo ve kurum ismi revizyonu yapılmıştır. Rehberlerin içeriğinde, uygulama ve denetim usulünde herhangi bir değişiklik yapılmamıştır.

Bilgi ve İletişim Güvenliği Rehberi uyum zorunluluğu devam ediyor mu?
Devlet teşkilatı içerisinde yer alan tüm kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmelerden bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan kurum, kuruluş ve işletmeler, Rehber'de yer verilen usul ve esaslara uymakla yükümlüdür.

3. Bilgi ve İletişim Güvenliği Denetim Rehberi

Denetim faaliyetlerini gerçekleştirmekle yükümlü kurum ve kuruluşlar hangileridir?
Milli güvenliğin sağlanması kapsamında görev ve faaliyet yürüten kurum ve kuruluşlar hariç olmak üzere bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşların tamamı denetim faaliyetlerini gerçekleştirmekle yükümlüdür.

Siber Güvenlik Başkanlığı tarafından gerçekleştirilen gözetim faaliyetleri kapsamında hangi kurum ve kuruluşların olacağı her gözetim döneminde belirlenerek ilgililere duyurulmaktadır.

Denetim faaliyetlerini gerçekleştirmekle yükümlü kritik altyapı hizmeti veren işletmeler hangileridir?
Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda kritik altyapı sektörleri; "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma", "Bankacılık ve Finans" olarak tanımlanmaktadır. 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış olan Sektörel SOME Kurulum ve Yönetim Rehberi içeriğinde her bir kritik altyapı sektöründe faaliyet gösteren kurum ve kuruluşlar özelinde Sektörel SOME'ler yer almaktadır. Bu doğrultuda kritik altyapı sektörlerinde faaliyet gösteren işletmelerin, kritik altyapı hizmeti veren işletme özelliğinde olup olmadığı, ilgili Sektörel SOME'yi işleten kurumların tasarrufundadır. Dolayısıyla Sektörel SOME'leri işleten kurumlar tarafından Bilgi ve İletişim Güvenliği Rehberine uyum faaliyetlerini gerçekleştirmekle yükümlü tutulan kritik altyapı hizmeti veren işletmelerin tamamı Bilgi ve İletişim Güvenliği Denetim Rehberi doğrultusunda denetim faaliyetlerini gerçekleştirmeli ve denetim sonuçlarını Siber Güvenlik Başkanlığı'na iletmelidir.

Kamu kurum ve kuruluşlarında denetim ekibi nasıl oluşturulur?
Denetim ekibi en az 2 denetçiden oluşmalıdır. Denetimin kapsamı ve denetlenen sistemlerin karmaşıklığına bağlı olarak denetim ekibindeki denetçi sayısı artırılabilir.

Denetim ekibi kurum **iç kaynakları ile oluşturuluyor ise** aşağıda belirtilen yetkinliklerin en az birini haiz personelden oluşması gerekmekte olup; denetçilerden biri Denetim Koordinatörü olarak belirlenmelidir.

- İç tetkik veya iç denetim faaliyetlerinde bulunmuş ve bilgi sistemleri denetimi alanında eğitim almış
- ISO/IEC 27001 Başdenetçi sertifikasına sahip
- CISA sertifikasına sahip
- TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında yetkilendirilmiş denetçi veya başdenetçi

Denetim ekibi aşağıdaki öncelik sırasına göre oluşturulur.

- Kurum iç denetçisi
- Kurum içi personel (Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetlerinde yer almayan ve denetlenen birime bağlı olmayan personel)
- Diğer kamu kurum ve kuruluşlarından görevlendirilecek personel

Denetim ekibi hizmet alım yolu ile oluşturuluyor ise;

- Ekipte, TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında yetkilendirilen en az bir başdenetçi ve denetçi bulunmak zorundadır. Ekipteki başdenetçi aynı zamanda Denetim Koordinatörü'dür. Ekipte birden fazla başdenetçi olması durumunda başdenetçilerden biri Denetim Koordinatörü olarak görevlendirilir.

Kritik altyapı hizmeti veren işletmelerde denetim ekibi nasıl oluşturulur?

Denetim ekibi en az 2 denetçiden oluşmalıdır. Denetimin kapsamı ve denetlenen sistemlerin karmaşıklığına bağlı olarak denetim ekibindeki denetçi sayısı artırılabilir.

Denetim ekibi kurum iç kaynakları ile oluşturuluyor ise;

Aşağıda belirtilen yetkinliklerin en az birini haiz personelden oluşması gerekmekte olup; denetçilerden biri Denetim Koordinatörü olarak belirlenmelidir.

- ISO/IEC 27001 Başdenetçi sertifikasına sahip
- CISA sertifikasına sahip
- TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında yetkilendirilmiş denetçi veya başdenetçi

Denetim ekibi aşağıdaki öncelik sırasına göre oluşturulur.

- Kurum iç denetçisi
- Kurum içi personel (Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetlerinde yer almayan ve denetlenen birime bağlı olmayan personel)

Denetim ekibi hizmet alım yolu ile oluşturuluyor ise;

- Ekipte, TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında yetkilendirilen en az bir başdenetçi ve

denetçi bulunmak zorundadır. Ekipteki başdenetçi aynı zamanda Denetim Koordinatörü'dür. Ekipte birden fazla başdenetçi olması durumunda başdenetçilerden biri Denetim Koordinatörü olarak görevlendirilir.

Düzenleyici ve denetleyici kurumlar, kapsamı dâhilindeki kritik altyapı sektörlerinde hizmet veren kurum ve kuruluşlarda denetim faaliyetini gerçekleştirecek firma ve ekip için ilave yeterlilik ve yetkinlik kriterleri belirleyebilir.

Kurum ve kuruluşların Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetlerini yürütmekle sorumlu birim(ler)inde görev alan personel denetim faaliyetlerini yürütebilir mi?

Denetim faaliyetlerinin bağımsız ve tarafsız bir şekilde yürütülmesini teminen denetim ekibi Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetlerini yürütmekle sorumlu birim(ler)de görev almayan ve denetlenen birime bağlı olmayan personelden teşkil edilmelidir.

İlk yıl denetim faaliyetlerinin hizmet alım yolu ile gerçekleştirilmesi durumunda sonraki yıl denetimleri için nasıl bir yol izlemelidir?

İlk yıl denetim faaliyetlerinin hizmet alım yolu ile gerçekleştirilmesi durumunda, sonraki yıl denetimlerinin kurum/kuruluş iç kaynakları ile yürütülmesi için gerekli bütçe, personel vb. gereksinimlere yönelik planlamalar yapılmalıdır. Ancak, gerekli iç kaynak tesis edilemediği durumda sonraki yıl denetimlerinde de hizmet alım yolu ile denetimler gerçekleştirilebilir.

Denetim ekibinde denetçi dışında uzman personel yer alabilir mi?

Denetim çalışmalarında, denetim ekibindeki denetçilere ilave olarak özel uzmanlık veya ihtisas gerektiren alanlarda tecrübesinden faydalanılmak üzere uzman personel görevlendirilebilir. Denetim ekibinde uzman yer alması durumunda, uzmanın yapacağı çalışmalar denetçi refakatinde gerçekleştirilir. Uzmanın; hangi varlık grupları, tedbirler ya da süreçler üzerinde çalışma yapacağı, çalışmaların denetçiye nasıl raporlanacağı denetçiler tarafından belirlenir.

Kurum ve kuruluşlar iç kaynakları ile denetim faaliyetlerini gerçekleştiremediği durumda hangi firmalardan hizmet alabilir?

Kurum ve kuruluşlar, iç kaynakları ile denetim faaliyetlerini gerçekleştiremediği durumda denetim faaliyetlerini gerçekleştirmek üzere TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında belgelendirilen firmalardan hizmet alabilir. İlgili firmalara bu bağlantıdan erişim sağlanabilir.

Düzenleyici ve denetleyici kurumlar, kapsamı dâhilindeki kritik altyapı sektörlerinde hizmet veren kurum ve kuruluşlarda denetim faaliyetini gerçekleştirecek firma ve ekip için ilave kriterler tanımlayabilir.

Bilgi ve İletişim Güvenliği Rehberi kapsamında denetim faaliyetlerini gerçekleştirmek üzere yetkilendirilmiş firmaların gerekli belgelendirme şartlarını yerine getirmeye devam ettiğinin takibi nasıl yapılacaktır?

Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Firmaların gerekli belgelendirme şartlarını yerine getirmeye devam ettiğinin takibi TSE tarafından yapılmakta olup, sürece yönelik işleyiş "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirme Programı" içeriğinde yer almaktadır.

Kurum ve kuruluşlar Bilgi ve İletişim Güvenliği Rehberi konusunda danışmanlık aldıkları firmalardan denetim hizmeti alabilir mi?
Kurum ve kuruluşlar, hizmet alım sözleşmesi tarihinden önceki iki yıl içerisinde Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetleri konusunda danışmanlık hizmeti aldıkları firma ve denetçilerden hizmet alamazlar.

Kurum ve kuruluşlar, aynı firmadan denetim hizmetini en fazla kaç yıl alabilirler?
Kurum ve kuruluşlar aynı firmadan art arda en fazla üç denetim hizmeti alabilirler.

Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetlerini tamamlayamayan kurum ve kuruluşlar denetim sürecini nasıl gerçekleştirecektir?
Rehber uyum çalışmaları kapsamında yürütülen faaliyetlerin ve alınan tedbirlerin uygunluğunu belirlemek amacıyla kurum ve kuruluşlar tarafından yılda en az bir kez denetim çalışmalarının gerçekleştirilmesi beklenmektedir.

Rehber uyum çalışmalarına başlamayan veya varlık grupları ile varlık gruplarının kritiklik derecesini belirlemeyen kurum ve kuruluşlar, Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi üzerinden mevcut durumları ve planlamaları hakkında beyanda bulunmalıdır.

Varlık grupları ile varlık gruplarının kritiklik derecesini belirleyen kurum ve kuruluşlar, mevcut durumları kapsamında denetim faaliyetlerini gerçekleştirerek denetim sonuçlarını Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi üzerinden iletmelidir. Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi üzerinden veri girişi yapılacak tarih aralığı her yıl Siber Güvenlik Başkanlığı tarafından ilgililere duyurulmaktadır.

Bilgi ve İletişim Güvenliği Rehberi uyum denetimleri ile bilgi ve iletişim güvenliği konulu diğer denetimler birlikte yürütülebilir mi?
Kurum ve kuruluşlar hâlihazırda uymakla yükümlü olduğu mevzuat doğrultusunda ilgili olduğu sektörden sorumlu düzenleyici ve denetleyici kuruluş, ilgili bakanlık veya diğer otoriteler tarafından gerçekleştirmekle yükümlü tutulduğu bilgi ve iletişim güvenliği konulu denetimleri, Bilgi ve İletişim Güvenliği Rehberi uyum denetimleri ile örtüştürebildiği durumlarda bu denetimleri birlikte gerçekleştirebilir. Ancak denetim çalışmaları neticesinde Siber Güvenlik Başkanlığı'na iletilmesi gereken denetim sonuçları Bilgi ve İletişim Güvenliği Denetim Rehberi'nde tanımlı formatlara uygun olarak oluşturulmalıdır.

Kurum ve kuruluşlar, Rehber uyum süreci ile TS EN ISO/IEC 27001 uyumlu Bilgi Güvenliği Yönetim Sistemi (BGYS) süreçlerinin entegrasyonu ve BGYS iç tetkik çalışmaları ile Rehber uyum denetimlerinin tek bir denetim altında yürütülmesi çalışmalarında yararlanmak amacıyla TS EN ISO/IEC 27001 Standardının EK-A Referans Kontrol Amaçları ve Kontrolleri ile Bilgi ve İletişim Güvenliği Rehberinde tanımlanan tedbirler arasındaki ilişkiyi ortaya koyan eşleştirme tablosundan faydalanabilir.

Kurum ve kuruluşlar denetim sonuçlarını en geç hangi tarihe kadar Siber Güvenlik Başkanlığı'na iletmelidir?
Kurum ve kuruluşlar, denetim raporunun imzalanma tarihinden itibaren **iki ay içerisinde** sonuçları Siber Güvenlik Başkanlığı'na iletmelidir.

Kurum ve kuruluşlar, Siber Güvenlik Başkanlığı'na denetim raporunun hangi bölümlerini iletecektir?
Kurum ve kuruluşlar denetim raporunda yer alan

- Denetim Ekibi Bilgisi
- Varlık Grupları ve Denetim Kapsamı
- Rehber Uygulama Süreci Etkinlik Durumu
- Tedbir Etkinlik Durumu
- Denetim Görüşü

bölümlerini 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile Üst Yönetici veya Üst Yöneticinin yetkilendirdiği personel tarafından imzalayarak Siber Güvenlik Başkanlığı'na iletir.

Siber Güvenlik Başkanlığı'na denetim sonuçları nasıl iletilecektir?
Kurum ve kuruluşlar denetim sonuçlarını Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi üzerinden ileteceklerdir.

Bilgi ve İletişim Güvenliği Denetim Rehberi ile ilgili soru, görüş ve öneriler nasıl iletilebilir?
Bilgi ve İletişim Güvenliği Denetim Rehberi ile ilgili her türlü soru, görüş ve öneri bgrehber[@]siberguvenlik[.]gov[.]tr e-posta adresine iletilebilir.

TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında belgelendirilen firmalara nereden erişilebilir?
TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında belgelendirilen firmalara bu bağlantı üzerinden erişilebilir.

TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı ile ilgili ayrıntılı bilgiye nereden erişilebilir?
TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı ile ilgili ayrıntılı bilgiye bu bağlantı üzerinden erişilebilir.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi kapsamında yapılan denetimler devam edecek mi? Yaptırım uygulanacak mı?
2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, kamu kurumları ve kritik altyapı işletmeleri için yılda en az bir kez zorunlu denetim şartı getirmiştir. Denetimlerin Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak iç denetim yoluyla gerçekleştirilmesi beklenmektedir.

Millî güvenliğin sağlanması kapsamında görev ve faaliyet yürüten kurum ve kuruluşlar hariç olmak üzere bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşların tamamı denetim faaliyetlerini gerçekleştirmekle yükümlüdür.

Başkanlık tarafından gerçekleştirilen gözetim faaliyetleri kapsamında hangi kurum ve kuruluşların olacağı her gözetim döneminde belirlenerek ilgililere duyurulmaktadır.

Genelge ve Rehber'de yer alan tedbirlerin uygulanmasına ilişkin yapılacak denetimler bilgi güvenliğini sağlamayı amaçlamaktadır. Söz konusu tedbirlere uyulmaması nedeniyle bir zafiyet oluşması durumunda, 7545 sayılı Siber Güvenlik Kanunu ile sair mevzuatta belirlenen yaptırımlar geçerlidir. Oluşabilecek zararın boyutuna göre gerek duyulması durumunda kurum içi adli veya idari soruşturma süreçleri işletilebilecektir.

Denetim usul ve esasları Bilgi ve İletişim Güvenliği Denetim Rehberi'nde yer almaktadır.

Siber Güvenlik Başkanlığı 7545 sayılı Siber Güvenlik Kanunu çerçevesinde kurumlara denetim yapmakta mıdır?

7545 sayılı Siber Güvenlik Kanunu'nun 8'inci maddesinde "*Başkanlık, bu Kanunda belirtilen görevleri ile ilgili olarak gerekli gördüğü hallerde Kanunun kapsamına giren her türlü fiil ve işlemi denetleyebilir; bu amaçla mahallinde inceleme yapabilir veya yaptırabilir. Denetim, bu Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilerin bu Kanun hükümleriyle ilgili faaliyet ve işlemlerini kapsar (...)*" hükmü yer almaktadır. Bu doğrultuda Başkanlık; Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilerin mezkûr Kanun hükümleriyle ilgili faaliyet ve işlemler çerçevesinde denetim yetkisine sahiptir.

4. Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi

Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi (BİGDES) nedir?

BİGDES; bilgi ve iletişim güvenliği tedbirlerinin uygulanmasına, bilgi ve iletişim güvenliği tedbirlerinin uygulama sürecinin ve etkinliğinin denetimine ve bilgi güvenliği yönetim sisteminin kurulumu ve işletimine yönelik yürütülen faaliyetlerin gözetimini sağlamak amacıyla kullanılmaktadır.

Başkanlığımız 2019/12 sayılı Genelge kapsamındaki kurum ve kuruluşlar tarafından gerçekleştirilmesi gereken Bilgi ve İletişim Güvenliği Rehberi uyum denetimine ilişkin sonuçları BİGDES üzerinden almaktadır.

BİGDES'e nasıl erişilebilir?

BİGDES'e yalnızca Rehber kapsamındaki kurum ve kuruluşlar tarafından belirlenen Kurum Yetkilileri e-devlet hesapları ile erişebilmektedir.

BİGDES'te kullanıcı ekleme süreci nasıldır?

Kurum Yetkilisi olarak belirlenen personel için BİGDES'te kullanıcı açma talebi, Kurum Yetkilisi Formu eksiksiz doldurularak Başkanlığımız "siberguvenlikbaskanligi@hs01.kep.tr" KEP adresine veya Siber Güvenlik Başkanlığına fiziki posta aracılığıyla resmî yazıyla iletilmelidir.

Kurum Yetkilisi Formu doldurulurken dikkat edilmesi gereken hususlar:

- Personel e-posta adresi, kişiye özel kurumsal e-posta adresi olmalıdır. Bireysel e-posta adresleri sisteme kaydedilememektedir.
- Bir e-posta adresi yalnızca bir kişiye tanımlanabilmektedir. Dolayısıyla her bir Kurum Yetkilisi için ayrı e-posta adresi bilgisi iletilmelidir.

BİGDES Kurum Yetkilileri nasıl belirlenir, asgari yetkinlikleri nelerdir?

BİGDES'in kullanılabilmesi ve aynı zamanda bilgi ve iletişim güvenliği tedbirleri konusunda Başkanlığımız ile iletişim ve koordinasyon faaliyetlerinin sağlanabilmesi amacıyla Rehber kapsamındaki kurum ve kuruluşlar tarafından Kurum Yetkilileri belirlenmektedir. BİGDES Kurum Yetkililerinin asgari olarak;

- Bilgi ve iletişim teknolojileri konusunda en az 3 yıl tecrübeye sahip olması,
- Bilgi güvenliği alanındaki terminolojiye hâkim olması,
- Kurum organizasyon yapısı ile organizasyondaki birimlerin görevlerine hâkim olması,
- Uzman, proje yöneticisi, şube müdürü ve grup başkanı seviyesinde görev yürütüyor olması

gerekmektedir.

BİGDES Kurum Yetkililerinin görev ve sorumlulukları nelerdir?

- Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi'nde (BİGDES) Kurum Yetkilisi rolünü üstlenmek
- Kurum ve Siber Güvenlik Başkanlığı arasında bilgi ve iletişim güvenliği faaliyetleri ile ilgili irtibat noktası olarak iletişim ve koordinasyon faaliyetlerini yürütmek
- Bilgi ve iletişim güvenliği ile ilgili faaliyetlerin yürütülmesinden sorumlu birim(ler)in ve kullanıcıların BİGDES üzerinde tanımlanması ve güncelliğinin sağlanmasına yönelik çalışmaları yürütmek
- Siber Güvenlik Başkanlığı tarafından bilgi ve iletişim güvenliği tedbirleri kapsamında bildirilecek zafiyetlere ve siber olaylara karşı aksiyon alınması ve bu kapsamda yapılan çalışmaların sonuçlarının paylaşılması hususunda koordinasyon sağlamak

BİGDES'e yeni Kurum Yetkilisi personeli nasıl ekleyebiliriz?

Kurum Yetkilisi olarak belirlenen personel(ler)in görevli diğer personelleri ekleme, çıkarma ve güncelleme yetkisi bulunmaktadır.

Kurum Yetkilisi işten ayrıldı, yeni Kurum Yetkilisi nasıl ekleyebiliriz?

BİGDES'te kayıtlı mevcut Kurum Yetkili(leri)nizin tamamının işten ayrılması durumunda, yeni Kurum Yetkilisi tanımlanabilmesi için talebinizi içeren resmî yazının Siber Güvenlik Başkanlığı KEP adresi veya fiziki posta aracılığıyla gönderilmesi gerekmektedir.