TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

# DDO Bilgi ve İletişim Güvenliği Rehberi

# Uyum Danışmanlığı Hizmeti

**Gits Global İnovasyon Teknolojileri Yazılım ve Yönetim Danışmanlık A.Ş.**
İnkılap Mh. Kirazlı Sk. No:69 Kat:1-2-3 Global Plaza Ümraniye / İSTANBUL
Telefon : 444 2 499
Eposta: info@globalgrup.com.tr Web: www.globalkvkk.com

## İÇİNDEKİLER



*Ekler:*

## Yasal Mevzuat:

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır.

## Amaç:

Rehberin temel amacı;

- Bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle 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 yürütülecek faaliyetlerin tanımlanmasıdır.

## Hizmetin Kapsamı:

- Mevcut durum analizi yapılması,
- Sektörel risklerin belirlenmesi
- Varlık gruplarının belirlenmesi,
- Varlık gruplarının kritiklik derecesinin belirlenmesi,
- Mevcut durum ve boşluk analizi,
- Rehber uygulama yol haritasının hazırlanması,
- Kurum içinde ISO27001 Bilgi Güvenliği Yönetim Sistemi ile entegrasyon çalışması ve rehberlik
- Kurum içinde ISO27701 Kişisel Veri Güvenliği Sistemi ile entegrasyon çalışması ve rehberlik
- Kurum içinde KVKK Kanunu kapsamında entegrasyon sağlanması ve rehberlik
- Tüm çalışanlara "Farkındalık Eğitimi" verilmesi

## Hizmetin Kapsamı ve İçeriği

| | | |
|---|---|---|
| **VARLIK GRUPLARININ BELİRLENMESİ** | **Açıklama** | DDO Bilgi ve İletişim Güvenliği Rehberi kapsamında yürütülen çalışmalarda varlıkların belirlenen başlıklar altında toplanarak gruplandırılması ve bu gruplar dikkate alınarak tedbirlerin uygulanması gerekmektedir. Rehber; elektronik ortamda yer alan bilgi/verinin depolandığı, aktarıldığı, işlendiği bilgi işleme olanakları, bilgi işleme olanaklarını kullanan personel ile bilgi işleme olanaklarını barındıran fiziksel ortamlara ilişkin varlıkları kapsamaktadır. |
| | **Süreç Kapsamı** | • Ağ ve Sistemler<br>• Uygulamalar<br>• Taşınabilir Cihaz ve Ortamlar<br>• Nesnelerin İnterneti (IoT) Cihazları<br>• Fiziksel Mekânlar<br>• Personel |
| **VARLIK GRUBU KRİTİK DERECELERİN BELİRLENMESİ** | **Açıklama** | Varlık gruplarının belirlenmesinin ardından bu varlık gruplarının hangi kritiklik derecesine sahip olduğu belirlenecektir. Her bir varlık grubunun kritiklik derecesi, işlenen verinin gizlilik, bütünlük ve erişilebilirlik açısından kritikliği ile oluşabilecek güvenlik ihlallerinin etki alanları dikkate alınarak belirlenecektir. |
| | **Süreç Kapsamı** | İşlenen veri ile ilgili boyutlar<br>**Gizlilik:** Bilginin yetkisiz kişilerin erişimine karşı korunması<br>**Bütünlük:** Bilginin tam ve doğru olma durumunun korunması<br>**Erişilebilirlik:** Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması<br>• Etki alanı ile ilgili boyutlar<br>**Bağımlı Varlıklar:** Varlık grubuna bağımlı olan diğer varlıklar üzerindeki etkisi<br>**Etkilenen Kişi Sayısı:** Bilgi güvenliği ihlal olayı meydana geldiğinde etkilenebilecek kişi sayısı<br>**Kurumsal Sonuçlar:** Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak durum<br>**Sektörel Etki:** Varlık grubunun hizmet verdiği sektöre etkisi<br>**Toplumsal Sonuçlar:** Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak toplumsal durum |
| **ANKET UYGULAMASI** | **Açıklama** | "Varlık Grubu Kritiklik Derecelendirme Anketi" uygulanır |
| | **Süreç Kapsamı** | - Tanımlanan anket her bir varlık grubu özelinde rehber uyumluluk denetimi kapsamında kontrol edilir.<br>- İlgili varlık grubu için uygulanması gereken tedbir maddeleri, varlık grubu için belirlenmiş olan kritiklik derecesi göz önünde bulundurularak belirlenir. |

| | | |
|---|---|---|
| **MEVCUT DURUM ANALİZİ** | **Açıklama** | Kurum içinde IT süreçleri analiz edilir. |
| | **Süreç Kapsamı** | - Tanımlanan anket her bir varlık grubu özelinde rehber uyumluluk denetimi kapsamında kontrol edilir.<br>- İlgili varlık grubu için uygulanması gereken tedbir maddeleri, varlık grubu için belirlenmiş olan kritiklik derecesi göz önünde bulundurularak belirlenir. |
| **BOŞLUK TESTİ** | **Açıklama** | "Boşluk Testi" uygulanır |
| | **Süreç Kapsamı** | Varlık gruplarına yönelik güvenlik tedbirleri ana başlıkları:<br>• Ağ ve Sistem Güvenliği<br>• Uygulama ve Veri Güvenliği<br>• Taşınabilir Cihaz ve Ortam Güvenliği<br>• Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği<br>• Personel Güvenliği<br>• Fiziksel Mekânların Güvenliği<br>Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ana başlıkları:<br>• Kişisel Verilerin Güvenliği<br>• Anlık Mesajlaşma Güvenliği<br>• Bulut Bilişim Güvenliği<br>• Kripto Uygulamaları Güvenliği<br>• Kritik Altyapılar Güvenliği<br>• Yeni Geliştirmeler ve Tedarik<br>Sıkılaştırma faaliyetlerine yönelik güvenlik tedbirleri ana başlıkları:<br>• İşletim Sistemi Sıkılaştırma Tedbirleri<br>• Veri Tabanı Sıkılaştırma Tedbirleri<br>• Sunucu Sıkılaştırma Tedbirleri |
| **YOL HARİTASI HAZIRLANMASI** | **Açıklama** | Boşluk analizi sonucunda tespit edilen eksikliklerin giderilmesi için gereken faaliyetler belirlendikten sonra planlama yapılır. |
| | **Süreç Kapsamı** | - Yetkinlik kazanımı ve eğitimler<br>- Ürün tedariki<br>- Hizmet alımı<br>- Danışmanlık<br>- Geliştirme / yeniden geliştirme<br>- Tasarlama / yeniden tasarlama<br>- Sıkılaştırma<br>- Sürüm güncelleme<br>- Dokümantasyon<br>- Kurumsal süreç iyileştirme |