ULAŞTIRMA VE ALTYAPI BAKANLIĞI

KARAYOLLARI GENEL MÜDÜRLÜĞÜ

KARAYOLLARI GENEL MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKASI

"Hizmete Özel"

HAZIRLAYAN		
Bilgi Teknolojileri Dairesi Başkanlığı		
Doküman No: POL.01	Revizyon No: 03	Revizyon Tarihi: 13.12.2022

1. Amaç

KGM'ye bilgi güvenliğini yönetmekteki amacı; kurumsal bilgilerin uygun sınıflandırma düzeyinde gizlilik, bütünlük ve erişilebilirlik özelliklerinin temin edilmesi, içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunması ve bu amaçla yürütülen faaliyetlerin etkin, doğru ve güvenli bir şekilde gerçekleştirilmesini temin etmektir.

Bilgi güvenliği politikasının amacı ise, KGM bünyesinde bilgi güvenliği kurallarının oluşturulan dokümantasyon ile yazı hale getirilmesi ve tüm ilgili taraflara KGM bilgi güvenliği gereksinimlerinin bildirilmesi ve yazılı kuralların temel dayanağının oluşturulmasıdır.

2. Kapsam

Bu politika tüm KGM'ye kapsamakla birlikte Bilgi Teknolojileri Dairesi Başkanlığında Bilgi Güvenliği Yönetim Sistemi kurulmuş ve uygulanmaktadır.

KGM Bilgi Teknolojileri Dairesi Başkanlığının sunduğu hizmetler ile ilgili tüm faaliyetler kapsam dâhilindedir.

KGM BGYS'si kapsamında aşağıdaki çalışma ortamları bulunur:

- Karayolları Genel Müdürlüğü İnönü Bulvarı No: 14 Yücetepe/ANKARA adresinde yerleşik olan Genel Müdürlük Kampüsü içerisinde bulunan Bilgi Teknolojileri Dairesi Başkanlığı çalışma ofisleri ve sistem odası kapsam dâhilinde değerlendirilmektedir.

KGM Bilgi Güvenliği Yönetim Sistemi aşağıdaki varlık kategorilerini kapsamaktadır:

- KGM bünyesinde üretilen, işlenen ve iletilen tüm bilgi varlıkları (Kağıt ve elektronik ortamdaki dosyalar, dokümanlar, veri tabanları vb.),
- KGM bünyesinde geliştirilen veya tedarik edilen uygulama veya sistem yazılımlarından oluşan yazılım varlıkları,
- KGM bünyesinde barındırılan ve işletilen tüm fiziksel varlıklar (ağ cihazları, güvenlik cihazları, sunucu sistemleri, uydu sistemleri, bilgisayarlar, iletişim donanımı, veri depolama ortamlar vb.),
- Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
- KGM' de faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıkları,
- KGM faaliyetlerinin yürütülmesinde kullanılan süreçler,
- KGM bünyesinde bir probleme çözüm bulma ya da beliren bir fırsatı değerlendirmeye yönelik projeler.

3. Sorumluluk

KGM üst yönetimi, Bilgi Güvenliği Politikasına uyulması, BGYS'nin kaynak tahsisi ile desteklenmesi ve sürdürülmesinden birinci derecede sorumludur.

Bilgi Teknolojileri Dairesi Başkanı ve birim müdürleri, çalışanların Bilgi Güvenliği Politikası ve tüm Bilgi Güvenliği Yönetim Sistemi dokümantasyonunu özümsemesi ve politikaya uygun hareket etmelerinin sağlanması, birim ile ilgili güvenlik risklerin belirlenmesi, değerlendirilmesi ve gerekli aksiyonların alınmasından sorumludur.

KGM çalışanları Bilgi Teknolojileri Dairesi Başkanlığı tarafından kurulmuş ve işletilmekte olan Bilgi Güvenliği Yönetim Sistemi çerçevesinde bilişim olanakları kullanıcıları için belirlenmiş kurallara ve tedbirlere uymaktan sorumludurlar.

Bilgi Teknolojileri Dairesi Başkanlığı çalışanları;

- Bilgi Güvenliği Politikası ve diğer bilgi güvenliği dokümantasyonuna uygun davranmaktan,
- Bilişim sistemlerinin işletimi, geliştirilmesi ve yönetimi ile uygulama geliştirme aşamalarını Bilgi Güvenliği Yönetim Sistemi tarafından belirlenen şartlara göre yürütmekten,
- Güvenlik ihlallerini bildirmekten,
- Sözleşmeli tedarikçiler ve/veya iş ortakları, bu esasa ve bu esas ile yürürlüğe konularak uygulanan BGYS politika, prosedür ve talimatlarına uymaktan,

sorumludurlar.

4. Tanımlar

Bu esasta geçen;

KGM	**:** Karayolları Genel Müdürlüğü,
Genel Müdür	**:** KGM Genel Müdürü' nü,
BGYS	**:** ISO/IEC 27001: 2017 standardında tanımlanan Bilgi Güvenliği Yönetim Sistemi'ni,
Bilgi Güvenliği	**:** KGM bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasını,
Bilgi Güvenliği Yönetim Temsilcisi	**:** KGM bünyesinde bilgi güvenliğinin uygulanması ve iyileştirilmesine ilişkin koordinasyonunu sağlayan insan kaynağını,
Bilgi İşleme Altyapısı	**:** Bilgi işlenmesi sırasında kullanılan bilgisayar donanım, yazılım, bilgisayar ağları ve insan kaynaklarını,
Bütünlük	**:** Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması özelliğini,
Erişilebilirlik	**:** Bilginin ihtiyaç duyulduğu an erişilebilir olması özelliğini,
Gizlilik	**:** Bilginin sadece yetkilendirilmiş kişiler tarafından görülebilir olması özelliğini,
İlgili taraflar	**:** KGM'nin iş yaptığı ve yasal olarak sorumlu olduğu tarafları,
Kullanıcı	**:** Bilişim altyapısını ve hizmetlerini kullanan çalışanları,

ifade eder.

5. Bilgi Güvenliği Politikası

Karayolları Genel Müdürlüğü Bilgi Teknolojileri Dairesi Başkanlığı olarak, iş sürekliliğimize ve bilgi varlıklarımıza yönelik her türlü riski yönetmek amacıyla;

- Bilgi güvenliği Yönetim Sistemimizin ISO 27001:2017 standardının gereklerini yerine getirecek şekilde sürekli iyileştirip işleterek,
- Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uyarak,
- Bilgi varlıklarına yönelik riskleri sistematik olarak yöneterek,
- Çalışanların bilgi güvenliği farkındalığını artırarak,
- Kamu kurum ve kuruluşları içerisinde bilgi güvenliği açısından örnek bir kuruluş olmak için özveri ile çalışmayı taahhüt ederiz.

6. Referanslar

6.1. KGM Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde üretilen, işlenen, depolanan ve dağıtılan tüm bilgilerin gizlilik sınıflandırması "Varlık ve Risk Yönetim Prosedürü"ne göre yapılacak ve bu sınıflandırmaya göre gizli ve hassas bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin uygun şekilde sağlanması için gerekli kontroller uygulanacaktır.

6.2. KGM Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde kurumsal bilgi güvenliği varlıkları ve riskleri "Varlık ve Risk Yönetimi Prosedürü"ne göre sahiplendirilecek ve bu risklerin azaltılmasında sorumluluk öncelikli olarak varlık sahipleri ve risk sahiplerinde olacaktır.

6.3. KGM Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde Bilgi Güvenliği Yönetim Sistemi içerisinde bilginin gizlilik sınıflandırmasına uygun şekilde korunabilmesi için "Varlık ve Risk Yönetimi Prosedürü"ne göre riskler belirlenerek analiz edilecek ve kabul edilebilir seviye üzerinde kalan riskler güvenlik kontrolleri uygulanarak bu seviyenin altına indirilmeye çalışılacaktır.

6.4. KGM Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde kurumsal bilgilere erişim "Erişim Denetim Politikası"na göre yetkilendirme dâhilinde uygun şekilde kontrol edilecek, KGM tarafından belirlenmiş esaslara göre sağlanacak ve kurumsal bilgiler yetkisiz erişim girişimlerine karşı korunacaktır.

6.5. Yasal düzenlemeler (Kanunlar, yönetmelikler, genelgeler, tebliğler vb.) ve sözleşmelerden doğan gereksinimler "Yasal Mevzuata Uyum Prosedürü" ne göre karşılanacak, bunlarla uyumlu çalışma konusunda gerekli tedbirler alınacak ve çalışmalar yapılacaktır.

6.6. Kritik iş süreçlerini doğal felaketler ve işletim hatalarının etkilerinden korumak amacıyla bilgi güvenliğine yönelik olarak iş sürekliliği yönetimi "Bilgi Güvenliği İş Sürekliliği Yönetimi Prosedürü"ne göre uygulanacaktır.

6.7. Personelin bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına ve işe yeni başlayan çalışanlara "İnsan Kaynakları Güvenliği Prosedürü"ne göre verilecektir.

6.8. Bilgi güvenliğine yönelik gerçek ya da şüpheli tüm ihlaller rapor edilecek; ihlallere sebep olan uygunsuzluklar ve bunların kök sebepleri tespit edilecek, bunların tekrar etmesini engelleyici önlemler "Siber Olaylara Müdahale Prosedürü"ne göre alınacaktır.

6.9. Çalışma alanlarında, gizlilik dereceli ve hassas bilgiler açıkta bırakılmayacak ve bu bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler "Temiz Ekran ve Temiz Masa Politikası"na göre alınacaktır.

6.10. KGM çalışanları kullandıkları tüm bilgi sistemlerinde, "Parola Politikası"na göre KGM tarafından belirlenmiş olan kriterlere uygun parola kullanmakla sorumludur.

6.11. KGM çalışanları kurum ağ ve internet sistemlerini kullanırken KGM tarafından belirlenmiş olan kurallara "İnternet, Ağ ve Sosyal Medya Kullanım Politikası"na göre uygun hareket etmekle sorumludur.

6.12. KGM Bilgi Teknolojileri Dairesi Başkanlığı ilgili taraflarla (yüklenici, tedarikçi, müşteri, vb.) yaptıkları çalışmalarda "Üçüncü Taraf ve Tedarikçi İlişkileri Politikası"na göre gizlilik hususlarına dikkat edilecek ve kurumsal bilgilerin korunması amacıyla kurumsal gizlilik sözleşmesi imzalanacaktır.

6.13. KGM bünyesindeki bilgi işleme donanımlarının ve olanakları kullanımları, "Bilişim Olanakları Kullanım ve Yetkilendirme Prosedürü"nde belirlenen esaslara uygun şekilde yapılacaktır.

6.14. KGM Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde geliştirilen yazılımlar güvenli yazılım geliştirme uygulamalarına uygun şekilde "Güvenli Yazılım Geliştirme Prosedürü"ne göre geliştirilecek ve gerek hazır temin edilen yazılımlar gerekse geliştirilen yazılımlar güvenlik testlerinden geçirildikten ve tespit edilen açıklıkları kapatıldıktan sonra kullanılmaya başlanacaktır.

6.15. KGM çalışanları e-posta hizmetlerinin kullanımında "E-Posta Kullanım Politikası" na göre uygun şekilde hareket edeceklerdir.

6.16. Tüm birim yöneticileri, birim çalışanlarınca bu esaslara uyulması konusunda birinci derecede sorumlu olup, personelinin esaslara uygun olarak çalışmasını sağlamakla sorumludur.

6.17. Bu politikada belirtilen esasların konuya özgü detayları KGM bilgi güvenliği alt politikaları ve bilgi güvenliği prosedürlerinde verilmiştir.

7. Gözden Geçirme ve Sürekli İyileştirme

Bilgi Güvenliği Politikaları; değişiklikler, iş şartları, yasal ve teknik düzenlemeler ile ilgili gereksinimlerin değişmesi durumunda, bunlara uyum sağlamak amacıyla yılda en az bir (1) kez gözden geçirilir.