1. AMAÇ:

Bu politikanın amacı, "Kapsam Analizi Dokümanı"nda belirtilen süreçler içerisinde BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin yönlendirmesi, iç ve dış tarafların her türlü bilgi güvenliği yönetim sistemi gereksinimlerine ilişkin Sivil Havacılık Genel Müdürlüğü'nün bilgi güvenliği yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. KAPSAM:

Bu politikanın gereklilikleri, elektronik veya basılı formlardaki BGYS ile ilgili tüm politikalara, prosedürlere, formlara, kayıtlara vb. dokümanlara uygulanır. BGYS kapsamına dâhil olan birimler ve ilgili kapsam detayları, BGYS Kapsam Analizi Dokümanında tanımlanmıştır. Bu politika BGYS kapsamı dahilindeki çalışanları ve bilgi varlıklarını kapsamaktadır. BGYS kapsamı dahilindeki tüm çalışanlar, bu politikaya uymakla yükümlüdür.

3. HEDEFİ:

Bu politikanın hedefi; bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunmasını, bilgi güvenliği risklerinin etkin şekilde yönetilmesini, yasal ve düzenleyici gerekliliklere uyum sağlanmasını ve bilgi güvenliği farkındalığının artırılmasını sağlayarak güvenli ve sürdürülebilir bir bilgi güvenliği yönetim yapısı oluşturmaktır. Bilgi güvenliği hedefleri bu politika ile uyumlu, ölçülebilir ve izlenebilir şekilde belirlenir. Hedefler, sorumluları, terminleri ve değerlendirme yöntemleri ile birlikte BGYS Hedef Takip Listesinde tutulur, üç ayda bir BGYS Yürütme Komitesince izlenir ve Yönetimin Gözden Geçirmesinde değerlendirilir.

4. SORUMLULAR:

Üst Yönetim, BT Departman Yöneticisi, Bilgi Güvenliği Sorumlusu, süreç ve varlık sahipleri ile tüm çalışanlar; bilgi güvenliği politikasının uygulanması, sürdürülmesi, izlenmesi, güncel tutulması ve belirlenen bilgi güvenliği kurallarına uyulmasından sorumludur.

5. ETKİLEDİĞİ SÜREÇLER/PROSEDÜRLER:

Bilgi güvenliği, risk yönetimi, varlık yönetimi, erişim yönetimi, insan kaynakları güvenliği, olay yönetimi, iş sürekliliği, tedarikçi yönetimi, değişiklik yönetimi ve BT hizmet yönetimi süreçlerini etkiler.

6. ETKİLENDİĞİ SÜREÇLER/PROSEDÜRLER:

Risk yönetimi, yasal ve düzenleyici gereklilikler, iç tetkik, ölçme ve değerlendirme, doküman ve kayıt yönetimi, iş sürekliliği, varlık yönetimi ve tedarikçi yönetimi süreçlerinden etkilenir.

7. POLİTİKA GİRDİLERİ:

ÜST YÖNETİM TAAHHÜDÜ

Sivil Havacılık Genel Müdürlüğü Üst Yönetimi, BGYS sürecinde kurumun hedef ve politikalarını gerçekleştirmek için ISO/IEC 27001'de yer alan tüm gereksinimlerin yerine getirilecek şekilde kurulmasını ve işletilmesini taahhüt eder.

Sivil Havacılık Genel Müdürlüğü Üst Yönetimi, yayımlanmış ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları ve gerekli altyapı yatırımlarını tahsis edeceğini, sürecin etkinliğini sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

POLİTİKA

Sivil Havacılık Genel Müdürlüğü, verilerinin ve sistemlerinin yeterince korunması ve bilgi teknolojilerinin işleyişiyle ilişkili her türlü güvenlik riskinin yönetilmesi için yasal ve ticari sorumluluklara sahiptir. Sivil Havacılık Genel Müdürlüğü, bilgi ve iletişim sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak, güvenlik risklerini yönetmek, operasyonel, finansal ve işlediği kişisel verileri korumak için ISO 27001 Standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamayı hedefler.
ISO 27001 Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uygun olarak, risk bazlı düşünme yaklaşımı ile gerçekleştirdiğimiz ve sürekli iyileştirdiğimiz süreçlerimiz sayesinde, sunduğumuz hizmetlerin kamunun ihtiyaç ve beklentilerini karşılanmasını, paydaşlarımız, çalışanlarımız ve tedarikçilerimizin bilgilerinin gerekli şekilde korunmasını taahhüt edip güvence altına almaktayız.

Sivil Havacılık Genel Müdürlüğü Genel Müdür tarafından onaylanmış olan bu Bilgi Güvenliği Politikasının amacı;

- Bilgi Güvenliği Yönetim Sistemi kapsamında, kurumsal bilgi varlıklarının ve tüm ilgili taraflardan emanet edilen bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak,
- Bilginin Gizlilik, Bütünlük, Erişilebilirlik ile ilgili ortaya çıkabilecek risklerini değerlendirmek ve bu risklerin etkilerini en aza indirmek,
- Bilgi güvenliği ile ilgili tüm yasal mevzuat ve üçüncü taraflar ile yapılan sözleşmelere uymak,
- Yönetim Sisteminin gerekliliklerini karşılamak ve etkin bir şekilde işletmek üzere çalışanların yetkinliğini artıracak gerekli kaynakları ayırmak ve eğitim programları planlamak,
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçmek, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmek,
- Personelin yönetim sistemlerine katılımını ve uyumunu sağlamak için bilinçlendirici ve yönlendirici faaliyetler planlamak,
- Bilgi Güvenliği Yönetim Sisteminin yürütülmesi için kullanılan süreç ve faaliyetlerin sürekli iyileştirilmesi amacıyla düzenli gözden geçirmeler gerçekleştirmek,
- Bilgi güvenliği kontrollerini zorunlu tutan konulara ilişkin politikalar ve prosedürler hazırlamak, bu politikalara ve prosedürlere uyumluluğu gözden geçirmek, geliştirilmesi ve iyileştirilmesi için kontroller yapmak,
- Tüm iş süreçlerinin bilgi güvenliği süreçleriyle uyumlu ve dengeli olmasını sağlamaktır.

Kurum bünyesindeki BGYS kapsamında yayımlanan tüm dokümanlar, Bilgi Güvenliği Politikasını destekler. Bilgi Güvenliği Yöneticisi bu politikanın sürdürülmesinden ve politikanın gerçekleştirilmesi konusunda tavsiyelerde bulunmaktan, yol göstermekten doğrudan sorumludur ve yetkili otoritedir.

8. Dahili Dokümanlar

- Kapsam Analizi Dokümanı

9. REFERANS DOKÜMANLAR:

1. ISO/IEC 27001:2022 Bilgi güvenliği, siber güvenlik ve gizlilik koruması- Bilgi güvenliği yönetim sistemleri- Gereksinimler

Revizyon Takip Listesi	Revizyon Tarih	Açıklama
	12.10.2026	1.0

HAZIRLAYAN	UYGUN GÖREN	ONAYLAYAN