DEVLET HAVA MEYDANLARI İŞLETMESİ

GENEL MÜDÜRLÜĞÜ

Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Politikası

Doküman Kontrolü

Doküman Başlığı	Bilgi Güvenliği Politikası
Doküman No	-
İlk Yayın Tarihi	8.10.2018
Rev No	-
Son Revizyon Tarihi	-
Referans	ISO 27001:2013/A.5.1.1 - A.5.1.2 - Madde 5.2 - Madde 5.3

Revizyon Geçmişi

Rev. No.	Revizyon Tarihi	Revizyon Yapan	Revizyon Açıklaması

Doküman Onayları

Hazırlayan	Kontrol Eden	Onaylayan
Yasemin GÖKALP BGYS Sorumlusu	Akif GÖÇMEN BGYS Yöneticisi	Mehmet ATEŞ Genel Müdür V.

İÇERİK

1 AMAÇ

Bu politikanın amacı Devlet Hava Meydanları İşletmesi Genel Müdürlüğü'nde yürütülen Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bilgi güvenliğini sağlamak için uygulanacak temel politikaları ortaya koymak, bilgi güvenliği için genel bir çerçeve oluşturmak ve üst yönetimin bilgi güvenliğine verdiği desteği açık olarak ifade etmektir.

2 KAPSAM

Bu politika, Devlet Hava Meydanları İşletmesi Genel Müdürlüğü'nde yürütülen BGYS için Bilgi Güvenliği Kapsam Dokümanı'nda tanımlanan kapsamın tamamında geçerlidir.

3 TANIMLAR

Kuruluş: Devlet Hava Meydanları İşletmesi Genel Müdürlüğü

Paydaş: Devlet Hava Meydanları İşletmesi Genel Müdürlüğü kapsamında yürütülen faaliyetlerden olumlu veya olumsuz bir şekilde doğrudan veya dolaylı bir şekilde etkilenecek Kuruluşlar, gruplar veya kişilerdir.

Üçüncü Taraf: Kuruluşa sözleşme ile hizmet sağlayan tüzel kişiler ve personel.

Personel: Kuruluşta çalışan memur ve/veya sözleşmeli personel

Bilgi Güvenliği: Kuruluş varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunması

BGYS: Bilgi Güvenliği Yönetim Sistemi

BTDB: Bilgi Teknolojileri Dairesi Başkanlığı

BT: Bilgi Teknolojileri

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmesine karşı korunması ve değiştirildiğinde farkına varılmasıdır.

Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olmasıdır.

Varlık: Kuruluş için değerli olan ve bu nedenle uygun şekilde korunması gereken unsurlardır.

Varlık Sahibi: Sahip olduğu varlıkları yönetmekten ve kontrol etmekten sorumlu olan kişidir. Örneğin, personel tarafından kullanılan bilgisayarların varlık sahibi Bilgi Teknolojileri Dairesi Başkanlığı'dır.

DMK: Devlet Memurları Kanunu

KİT: Kamu İktisadi Teşebbüsleri Personel Rejiminin Düzenlenmesi

4 KURULUŞUN STRATEJİK YAKLAŞIMI

Kuruluş Misyonu

Havacılık sektöründe uluslararası standartlarda, kaliteli, güvenli, konforlu, insana ve çevreye duyarlı ileri teknoloji ürünü alt yapı ve sistemlere ve yetişmiş insan gücüne dayalı hava seyrüsefer ve havaalanı işletme hizmetleri sunmaktır.

Kuruluş Vizyonu

Hava trafik yönetimi ve havaalanı işletmeciliği alanında, küresel boyutta rekabet gücüne haiz dünyanın öncü Kuruluşlarından biri olmaktır.

5 BİLGİ GÜVENLİĞİ İHTİYACI

Kuruluşu bilgi güvenliğine yönelik içeriden ve dışarıdan gelebilecek saldırılara karşı korumak, Kuruluş için değerli bilgileri korumak ve gerçekleştirilen faaliyetlerde bilgi güvenliğini sağlamak ancak bilgi güvenliği uygulamaları ile mümkün olabilir.

Bilgilere yönelik risklere karşı etkin önlemler geliştirebilmek, Kuruluş hizmetlerinin en az kesinti ile sürdürülebilmesini sağlamak ve olası bilgi güvenliği olayları sebebiyle Kuruluş itibarının bozulmasını engellemek amacıyla, Kuruluşta bir Bilgi Güvenliği Yönetim Sistemi kurulmuştur.

BTDB, Kuruluş bilgi teknolojileri altyapısının kurulması ve yönetilmesinden sorumludur. Buna bağlı olarak, Kuruluşun bu altyapı üzerindeki bilgi güvenliği uygulamaları da BTDB tarafından yürütülmektedir.

6 BİLGİ GÜVENLİĞİ AMAÇLARI

Kuruluş, BGYS ile sahip olduğu bilgilerin ve sunduğu BT hizmetlerinin güvenliğini aşağıdaki unsurlar doğrultusunda sağlamayı hedefler:

- Personel, paydaş ve üçüncü tarafların bilgi güvenliği farkındalıklarını arttırmak.
- Bilgilerin güvenliği için etkin teknik güvenlik kontrollerini uygulamak.
- Kuruluşun temel ve destekleyici BT esaslı iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak.
- Bilgi güvenliğine ilişkin riskleri göz önünde bulundurarak, Kuruluşun güvenliğini, güvenilirliğini ve imajını korumak.
- Kuruluş tarafından üretilen, kullanılan, işlenen, iletilen, paylaşılan, saklanan sayısal ortamdaki bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak.
- Kuruluş tarafından geliştirilen sistemlerin, uygulamaların, yazılımların bilgi güvenliği gereksinimlerini karşılamak
- Kuruluş sistemleri üzerinden gerçekleşen tüm sayısal bilgi paylaşımı ve yararlanıcı işlemlerinin güvenliğini ve güvenilirliğini sağlamak.

- Kuruluşun tabi olduğu mevzuat, yasa ve yönetmeliklerin gerekliliklerinin karşılanmasını sağlamak.
- Paydaşlar ve üçüncü taraflar ile yapılan sözleşmelere uyumu sağlamak.

Kuruluş yukarıda belirtilen bilgi güvenliği amaçlarını sağlamak için BGYS Hedeflerini belirlemekte, bu hedeflere yönelik planlamaları yapmakta ve hedeflerin başarımını takip etmektedir. Bu hedefler üst yönetim ve BGYS Yöneticisi tarafından belirlenir, planlanır ve BGYS Sorumlusu tarafından takip edilir. Bu hedeflerin belirlenmesinde girdi olarak Risk Değerlendirme sürecinin çıktıları değerlendirilir. Bu sürecin detayı Risk Değerlendirme ve İşleme Prosedürü dokümanında belirtilmiştir.

7 BİLGİ GÜVENLİĞİ POLİTİKASI

Bu politika, Kuruluş bilgilerinin gizliliğinin, bütünlüğünün, erişilebilirliğinin korunması ve iş süreçlerinin sürekliliğinin sağlanması için uygulanmaktadır. Bu çerçevede bilgi güvenliği esasları aşağıda belirlenmiştir.

- Kuruluş bilgileri, gizlilik derecesine ve Erişim Yönetimi Politikasına uygun olarak, yetkisiz erişime karşı korunur ve yetkisiz kişilere kasten veya dikkatsizlik sonucu verilmez.
- Kuruluş bilgilerinin doğruluğu Erişim Yönetimi Politikasına uygun olarak, yetkisiz değişikliklere karşı koruma ile sağlanır.
- Kuruluş bilgileri, gereksinim duyulduğunda yetkili kullanıcıların erişimine hazır bulundurulur.
- Kuruluş kritik iş faaliyetleri, İş Sürekliliği Politikası'na uygun olarak, büyük felaketler ve işletim hatalarının etkilerinden korunur ve en az kesinti ile devam etmesi sağlanır.
- Kuruluşa ziyaretçi olarak gelen üçüncü taraflar, Kuruluş bilgi güvenliği politikaları hakkında bilgilendirilir ve bu politikalara uygun davranırlar.
- Kuruluşun tabi olduğu mevzuat, yasa ve yönetmeliklerin şartları yerine getirilir.
- Kuruluşun güvenilir imajı korunur.
- Paydaşlar ve üçüncü taraflarla yapılan sözleşmelere uygun hareket edilir.
- Kuruluşu olumsuz etkileyebilecek bilgi güvenliği riskleri, Risk Değerlendirme ve İşleme Prosedürü'ne uygun olarak kabul edilebilir düzeylere indirilir.
- Tüm birimler, bilgi güvenliği ile ilgili tüm prosedür ve politikalara uygun hareket eder. Bilgi güvenliği ile ilgili tüm dokümanları Kuruluş intranetinden erişilebilirdir.
- Tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimi verilir.
- Kuruluşta bilgi güvenliği ile ilgili tüm iletişimler BGYS İletişim Listesi dokümanına uygun olarak gerçekleştirilir.
- Tüm personel, haberdar oldukları bilgi güvenliği olaylarını BGYS Ekibine bildirmekle yükümlüdürler. Bilgi güvenliği olayları ile ilgili açıklamalar ve bildirim yöntemleri Bilgi Güvenliği Olay Yönetim Politikası'nda açıklanmıştır.

8 ÜST YÖNETİMİN BİLGİ GÜVENLİĞİ LİDERLİĞİ

BGYS'nin kurulması ve işletilmesi amacıyla Bilgi Güvenliği Yönetim Sistemi Yöneticisi, Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve BGYS Ekibi atanmış ve sorumlulukları tanımlanmıştır. BGYS'nin kurulması ve işletimi için gerekli tüm kaynaklar üst yönetim tarafından sağlanmaktadır.

BGYS kapsamında oluşturulan politika ve prosedürler Kuruluşta bilgi güvenliğinin sağlanması için uyulacak kuralları ve işletilecek süreçleri ortaya koymaktadır. Tüm personelin bu politika ve prosedürlere uyması ve bu doğrultuda hareket etmeleri gerekmektedir. Bilgi güvenliği politikaları ve süreçleri, Kuruluşta yürütülen diğer faaliyetlerle eşit öneme sahip olup bu süreçlerle bütünleşik olarak yürütülecektir. Tüm Daire Başkanları ve Şube Müdürleri, BGYS politika ve prosedürlerinin kendi birimlerinde uygulanmasını sağlamaktan sorumludur.

BGYS'nin geliştirilmesi ve iyileştirilmesi BGYS Ekibi'nin olduğu kadar tüm personelin sorumluluğundadır. Herkesin bu sistemin iyileştirilmesine katkı sağlayacak önerilerde bulunması beklenmektedir.

Bu şartlara, BGYS politika ve prosedürlerine uyulmaması durumunda aşağıda yer alan "Politikanın İhlali ve Yaptırımlar" maddesine göre yaptırımlar uygulanacaktır.

9 GÖREVLER VE SORUMLULUKLAR

Kuruluş, bu politikayı oluşturur, uygulanmasını sağlar ve gözden geçirir. BGYS Yöneticisi, BGYS'nin işleyişinin izlenmesinden ve sürekliliğinin sağlanmasından sorumludur. Ayrıca Kuruluş, BGYS'nin kurulmasından, işletilmesinden, altyapısını desteklemekten, işleyişini izlemek ve denetlemekten sorumludur. Kuruluş, BGYS'nin ISO/IEC 27001 standardına uygun olarak yürütülmesini sağlamak amacıyla BGYS Yöneticisi ve BGYS Ekibi'ni atamıştır. BGYS kapsamında ilgili personelin rol ve sorumlulukları görevler ayrılığı ilkesine uygun olarak belirlenmiş ve Roller ve Sorumluluklar Dokümanı'nda tanımlanmıştır. Bilgi güvenliği ile ilgili tüm personeli ilgilendiren sorumluluklar aşağıda tanımlanmıştır:

- Personel Güvenlik Taahhütnamesini imzalayarak Bilgi Güvenliği Politikası çerçevesinde belirlenen politika, prosedür ve talimatlara uyar.
- Görev tanımlarına bağlı olarak çalışma saatleri ve çalışma alanı dışında da mevcut görev ve sorumluluklarının gereği olan yükümlülüklere uyar. Herhangi bir bilgi güvenliği zaafiyetini veya olayını farkettiğinde, zaman geçirmeden "Bilgi Güvenliği Olay Yönetim Politikası'na uygun olarak Bilgi Güvenliği Ekibi'ne bildirir.
- Erişim izni olan bilişim hizmetlerini, ortak alanları, erişim yetkileri ve iş süreçlerine uygun olarak kullanır.
- Kurumsal bilgi varlıklarını, ağ ortamındaki sunucular üzerindeki ortak alanlarda bulundurarak, yedeklenmesini sağlar.
- Yetkisinde olan hesapların, şifrelerin, bilgi varlıklarının güvenliğini ve gizliliğini sağlar.

- "Çok Gizli" ve "Gizli" etiketli bilgilerin birim amiri onayı olmaksızın kopyalanmasına veya paylaşılmasına izin vermez.
- Belirlenen standart programlar dışında güvenliği zaafiyete uğratabilecek yazılım ve donanımları bilgisayarına kurmaz veya kurulumunu talep etmez.
- Lisanssız programları bilgisayarına kurmaz ve kurulumunu talep etmez.
- Kuruluş tarafından sağlanan her türlü yazılım, donanım ve iletişim kaynaklarını görev tanımı çerçevesinde kullanır.
- Elektronik iletişim ortamında, kişisel bilgisayar ve/veya yerel ağ disk alanlarında suç unsuru oluşturan her türlü bilgi, belge, resim, film, ses ve benzeri dosyaları bulundurmaz.
- Kullanıcının kişisel ortamında, belirlenen standartlar dışında var olabilecek fikir ve mülkiyet hakları ile korunan her türlü medyanın sorumluluğunu üstlenir.
- Görev tanımının gerektirdiği ve Bilgi Teknolojileri Dairesi Başkanlığı tarafından uygun görüş alınması durumları hariç olmak üzere bilgisayarda tam yetkili kullanıcı olmayı talep etmez.
- Ofis ortamının boş bırakılması durumunda, ortamdaki bilgi varlıklarını yetkisiz kullanıma karşı koruyacak önlemleri (Uygun Kullanım Politikası, ekran koruyucu kullanımı vb.) alır.
- Şüpheli bir kişiye ve eşlik edilmeyen bir yabancıya rastlandığında, durumu Kuruluş güvenlik görevlisine bildirir.
- Yılda en az bir kere bilgi güvenliği farkındalık eğitimlerine katılır.

10 POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Kuruluş bilgi güvenliği politikalarını ve prosedürlerini ihlal eden personel, paydaş ve üçüncü taraflar için ilgili sözleşmelerde yer alan, 657 sayılı DMK'da 399 sayılı KİT'de ve buna bağlı olarak çıkartılan disiplin yönetmeliklerinde yer alan cezai yaptırımlardan bir veya birden fazla maddesi uygulanabilir.

11 UYUMLULUK

Tüm personel ve üçüncü taraflar bu politikaya uygun davranmaktan sorumludur. BGYS Yöneticisi de bu politikanın uygulanmasından, uygulamanın denetlenmesinden ve politika dokümanının güncel tutulmasından sorumludur.

12 GÖZDEN GEÇİRME VE REVİZYON

Bilgi Güvenliği Politikası, BGYS Sorumlusu tarafından periyodik olarak yılda bir kez gözden geçirilir. Bilgi güvenliği ile ilgili diğer politika ve prosedürlerdeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika üst yönetim tarafından onaylanır ve ilgili taraflara iletilir. Onaylanan politika intranette yayınlanır.

13 REFERANSLAR

- Bilgi Güvenliği Kapsam Dokümanı
- Uygun Kullanım Politikası
- Erişim Yönetimi Politikası
- Fiziksel ve Çevresel Güvenlik Politikası
- İş Sürekliliği ve Acil Durum Planı
- Yedekleme Prosedürü
- Risk İşleme Planı
- Risk Değerlendirme Raporu
- Risk Değerlendirme ve İşleme Prosedürü
- Bilgi Güvenliği Olay Yönetim Politikası
- İş Sürekliliği Politikası
- Uygulanabilirlik Bildirgesi
- Roller ve Sorumluluklar Dokümanı
- Mevzuat ve Kanunlar