

Sayı : MIP-E-100033-732-12/906
Konu : MIP Bilgi Güvenliği Politikası Hk.

29.03.2023

DAĞITIM YERLERİNE


Değerli Paydaşlarımız,

Bilgi güvenliği, iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve bilginin uygun bir şekilde korunması gerekir. Hizmet verilen kurum ve kuruluşların güvenini temin etmek ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliği önceliğimizdir.

MIP, Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 standardını uygulayarak kurumsal bilginin gizlilik, bütünlük ve erişilebilirliği ile ilgili ortaya çıkabilecek riskleri ve bu risklerin etkilerini en aza indirmeyi amaçlar.

Bu kapsam ve hedef ile “MIP Bilgi Güvenliği Politikası” web sitemizde yayınlanmış ve ekte bilgilerinize sunulmuştur.

Konunun tüm üyelerinize duyurulması hususunda, bilgi ve gereğini saygılarımızla rica ederiz.

 e-imzalıdır

Kemal Kerem KAVRAR
Ticari Grup Müdürü

EKLER: 1. MIP Bilgi Güvenliği Politikası.pdf

DAĞITIM:

Gereği:

Mersin Gümrük Müşavirleri Derneği
Mersin Ticaret Ve Sanayi Odası
Mersin Deniz Ticaret Odası
Mersin Ticaret Borsası
Mersin Vapur Donatanları Ve
Acenteleri Derneği

Bilgi:

TCDD Mersin Liman İşletmesi Kontrol Müdürlüğü

1. Amaç Kapsam ve Hedef

Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. Hizmet verilen kurum ve kuruluşların güvenini temin etmek ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliği önceliğimizdir.

MIP, Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 standardını uygulayarak kurumsal bilginin gizlilik, bütünlük ve erişilebilirliği ile ilgili ortaya çıkabilecek riskleri ve bu risklerin etkilerini en aza indirmeyi amaçlar.

MIP Bilgi Güvenliği Politikası; MIP'nin itibarının, güvenilirliğinin, bilgi varlıklarının korunması, temel ve destekleyici iş faaliyetlerinin mümkün olan en az kesinti ile devam etmesi amacıyla:

- Bilgi sistemlerinin sürekliliğini tam olarak sağlamayı,
- Çalışanların bilinç, farkındalık ve güvenlik gereksinimlerine uyum düzeylerini en üst seviyeye çıkarmayı,
- Üçüncü taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,
- Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi
- Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve saklanmasını,
- En güncel ve etkin teknik güvenlik kontrolleri uygulamayı, hedefler.

Her bir MIP çalışanı bu hedeflere katkı sağlamaktan sorumludur.

2. Üst Yönetim Taahhüdü

MIP Yönetim Kurulu etkili bir bilgi güvenliği yönetim yapısının tesis edilmesi amacıyla, bilgi güvenliği stratejisi ve yol haritasının belirlendiği Bilgi Güvenliği Politikasını onaylar ve uygulanmasını zorunlu tutar.

MIP Üst Yönetimi aşağıdaki konuların yerine getirilmesini taahhüt eder:

- Bilginin ve bilgi sistemlerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması,
- Bilgi varlıklarına yönelik risklerin tespit edilmesi ve yönetilmesi,
- Bilgi güvenliği standartlarının gerekliliklerinin yerine getirilmesi,
- Bilgi güvenliği ile ilgili tüm yasal mevzuata uyumun sağlanması,
- Bilgi Güvenliği Yönetim Sisteminin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirilmesi ve çalışmalarının gerçekleştirilmesi,
- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirilmesi,
- Bu politikaya bağlı diğer alt prosedürlerin/talimatların/süreçlerin Bilgi Teknolojileri Grup Müdürlüğü ve Bilgi Güvenliği Yönetim Sistemleri Komitesi tarafından hazırlanması ve yayınlanması.

3. Tüm MIP Çalışanlarının Sorumlulukları

MIP Bilgi Güvenliği Politikası, tüm çalışanlar için coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. MIP Personeli "Bilgi Güvenliği Yönetim Sistemi" kapsamında yayınlanmış olan politika ve prosedürlere uymakla ve olası güvenlik ihlallerini ve zafiyetlerini bildirmekle yükümlüdür.

Bu kapsamda MIP personeli;

- Kendilerine duyurulan Bilgi Güvenliği Politikasına ve prosedürlerine uymak,
- Kendi süreç ve sistemlerinin yönetimleri için oluşturacakları süreç, akış, talimat, kılavuz, form gibi dokümanlarda Bilgi Güvenliği belgelerine uyumu sağlamak,

- Bilgi Güvenliđi politikalarına ve/veya prosedürlerine uyumun sağlanmadığı veya bilgi güvenliđi ihlal olaylarında ilgili birime bildirmek,
- Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliđini tehlikeye atacak faaliyetlerde bulunmamak,
- Bilgi Güvenliđi dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Güvenliđi Yönetim Sistemleri Komitesine bildirmek.
- Bilgi ve kurumsal kaynaklarına iş ihtiyaçları ölçüsünde erişim talebinde bulunmak,
- Sahibi olunan varlığın ve Kişisel Verilerin, erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceđini tayin etmek,
- Varlık envanterini gözlemlemek ve güncelliđini sağlamak,
- Sahibi oldukları varlıkların Kişisel Verileri dahil olmak üzere sınıflandırmasını, güncellenmesini ve gözden geçirilmesini sağlamaktan sorumludur.

MIP personeli, gizli bilgilerin korunması ve MIP İş Etiđi İlkelerine de uymak zorundadır. Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almaktan ve MIP Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmaktan sorumludur.

4. Üçüncü Partilerin Sorumlulukları

MIP dışı personeli, stajyerleri, dış taraf kullanıcıları, konumları veya görevleri ne olursa olsun tüm iş süreçlerini MIP bünyesinde bilgilerin korunmasını gözetecek biçimde yapmaktan sorumludur.

MIP personeli olmayan fakat MIP bilgilerine erişim geređi olan üçüncü taraf hizmet sağlayıcıları ve bunlara bađlı destek personeli konumunda olan kişilerin, bu politikanın genel ilkelerine, güvenlik yükümlülüklerine bađlı kalması şarttır.

MIP'ye mal ve hizmet sağlayan üçüncü kişilerin ve bunların çalışanlarının uyması gereken bilgi güvenliđine ilişkin düzenlemeler ilgili sözleşmeler ve protokoller ile belirlenir.

Bunlar asgari aşağıdaki hususları kapsar:

- Sözleşmeler veya protokoller ile bildirilen bilgi güvenliđi kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen MIP Politika ve Prosedürleri 'ne uygun hareket etmek
- MIP'ye ait bilgi ve varlıklarını MIP onayı ve izni olmadan başkaları ile paylaşmamak
- MIP tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak
- Üçüncü partinin MIP ile çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev deđiştirilmesi söz konusu ise, bu durumu aynı gün içerisinde MIP'ye bildirmek ve yetkilerinin iptal edilmesini sağlamak
- MIP'nin onay ve izni olmadan, MIP'nin cihazlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydını almamak, resmini, videosunu çekmemek, veri güvenliđini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak
- MIP lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

5. Politika Sahipliđi

Bu politikanın ve ilgili standartların ve diđer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliđi Bilgi Güvenliđi Yönetim Sistemi Komitesi tarafından yürütülecektir.

Bilgi Güvenliđi Yönetim Sistemi Komitesi aşağıdakilerden sorumludur:

- Gerekli olduđunda bu politikanın ayrıntılı standartlar, prosedürler, süreçler ve talimatların desteklenmesini ve bunların gerek dođdukça kullanıma hazır olmasını sağlamak,

- Bařta Bilgi Gvenlięi Politikası olmak zere yayınlanmış olan politika/prosedr/sreç/talimat ile ilgili standarda uyumun periyodik olarak denetlemek ve raporlamak
- Politika gereklerinin tm alıřanlar ve tm dıř taraflara duyurulmasını saęlamak
- Bilgi gvenlięi ile ilgili genel ynetim erevesinin oluřturulması ve sreklilięinin saęlanması
- Bu politikanın gncellenmesini ve MIP ve tm dıř tarafların iřle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karřı karřıya olduęu risk ortamındaki ya da tehditlerdeki deęiřimleri yansıtmaya devam etmesini temin edecek řekilde devamlı gzden geirmek.

6. Politikaya Uyum, Denetim ve Yaptırım

Her birim yneticisi Bilgi Gvenlięi Politikasına uyumun saęlanması iin gerekli tedbirleri almak ve sistemlerini gzden geirmekten birinci derece sorumludur.

Bilgi Gvenlięi Politikası ihlalleri, MIP'nin risklere karřı ihtiya duyulan kontrollerin uygulanmaması neticesinde zarar grmesine, ayrıca Trk Ceza Kanuna gre de cezai sorumluluk doęurmasına ve maddi zararların tazmini sorumluluęuna sebep olabilecektir. Gerek gzetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Gvenlięi Politikası ihlalleri istihdama son verilmesine hatta adli ve cezai yasal iřlemler bařlatılmasına varıncaya kadar gidebilecek řirket ii disiplin cezaları ile sonulanabilecektir.

Bu politikanın uygulanması konusunda hep birlikte alıřılması, bilgilerimizin ve itibarımızın srekli olarak korunmasına ve iřimizin bařarisının devamlılıęının saęlanmasına yardımcı olacaktır.