Bilgi Güvenliği Politikası

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,
- Üçüncü taraflardan gelen her tür bilgi istem talebini yazılı bir biçimde almak ve değerlendirmek
- Bilgi Güvenliği politikalarına ve/veya prosedürlerine uyumun sağlanmadığı veya bilgi güvenliği ihlal olaylarında ilgili birime bildirmek,
- Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak,
- Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Güvenliği 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 erişilebileceğini tayin etmek,
- Varlık envanterini gözlemlemek ve güncelliğini sağlamak,
- Sahibi oldukları varlıkların Kişisel Verileri dahil olmak üzere sınıflandırmasını, güncellenmesini ve gözden geçirilmesini sağlamaktan sorumludur.

MIP personeli, gizli bilgilerin korunması ve MIP İş Etiği 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 gereği olan üçüncü taraf hizmet sağlayıcıları ve bunlara bağlı destek personeli konumunda olan kişilerin, bu politikanın genel ilkelerine, güvenlik yükümlülüklerine bağlı kalması şarttır.

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

Bunlar asgari aşağıdaki hususları kapsar:

- Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği 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'ye ait herhangi bir bilgi ve varlığın talep edilmesi durumunda bu talebi yazılı bir biçimde sunmak
- MIP tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak
- Üçüncü partinin MIP ile çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi 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 güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak
- MIP lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

5. Politika Sahipliği

Bu politikanın ve ilgili standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği Bilgi Güvenliği Yönetim Sistemi Komitesi tarafından yürütülecektir.

Bilgi Güvenliği Yönetim Sistemi Komitesi aşağıdakilerden sorumludur:

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

- Başta Bilgi Güvenliği Politikası olmak üzere yayınlanmış olan politika/prosedür/süreç/talimat ile ilgili standarda uyumun periyodik olarak denetlemek ve raporlamak
- Politika gereklerinin tüm çalışanlar ve tüm dış taraflara duyurulmasını sağlamak
- Bilgi güvenliği ile ilgili genel yönetim çerçevesinin oluşturulması ve sürekliliğinin sağlanması
- Bu politikanın güncellenmesini ve MIP ve tüm dış tarafların işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirmek.

6. Politikaya Uyum, Denetim ve Yaptırım

Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemlerini gözden geçirmekten birinci derece sorumludur.

Bilgi Güvenliği Politikası ihlalleri, MIP'nin risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri istihdama son verilmesine hatta adli ve cezai yasal işlemler başlatılmasına varıncaya kadar gidebilecek şirket içi disiplin cezaları ile sonuçlanabilecektir.

Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.