1. Bilgi Güvenliğinin Amacı, Kapsamı ve Konunun Yönetim Tarafından Benimsenmesi

RAM DIŞ TİCARET A.Ş. (RAM) ve iştirakleri kurumsal bilgiyi son derece değerli bir varlık olarak kabul etmektedir. Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. RAM, Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 standardını uygulayarak kurumsal bilginin Gizlilik, Bütünlük, Kullanılabilirlik ile ilgili ortaya çıkabilecek riskleri ve bu risklerin etkilerini en aza indirmeyi amaçlar.
RAM Yönetim Kurulu Başkanı özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:
• RAM bilgilerinin ve bilgi sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını,
• Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini,
• Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
• Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı,
• Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirmeyi ve çalışmalarını gerçekleştirmeyi,
• Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi,
• Bu politikaya bağlı diğer alt prosedürlerin Bilgi Güvenliği Yönetim Kurulu tarafından hazırlanmasını ve yayınlanmasını.
RAM'ın Bilgi Güvenliği Politikaları, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, RAM bilgilerini veya iş sistemlerini kullanan tüm RAM personeli için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve RAM bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

2. Tüm Çalışanların Sorumlulukları

Bilgi Güvenliğinin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; RAM'a ait bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması; ve bilgilerin ve sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm RAM ve dış kaynaklı personel ile stajyerleri konumları veya görevleri ne olursa olsun işlerini, bilgilerin RAM bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur.
RAM'a ait bilgilerin eksiksiz, doğru ve kullanılabilir durumda hazır olmasının sağlanmasının yanı sıra tüm RAM personeli, RAM Personel Yönetmeliği Kurallarında belirtilen gizli bilgilerin korunması ve RAM İş Ahlakı İlkelerine de uymak zorundadır.

RAM; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve tam uyumlu çalışmayı taahhüt eder.

3. Politika Sahipliği ve Bilgi Güvenliğinde Rehberlik Sağlanması

Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği Bilgi Güvenliği Yönetim Kurulu tarafından yürütülecek ve bu kurul, aynı zamanda politikanın tüm RAM bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.
Bilgi Güvenliği Yönetim Kurulu tüm çalışanların, Bilgi Güvenliği konularıyla ilgili uygun bilinçlenme düzeyinin oluşmasını sağlayacak uygun eğitimleri almalarını temin edecek ve genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik edecektir. Gerekli olduğunda bu politikanın ayrıntılı
standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlayacaktır. Ayrıca bu politika gereklerinin tüm çalışanlara (daimi veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır.
Bilgi Güvenliği Yönetim Kurulu Başkanı, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından ve sürekliliğinin sağlanmasından ve bu politikanın, güncel olarak yaşamasını ve RAM ve iştiraklerinin 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 geçirilmesinden sorumlu olacaktır.
Bilgi Güvenliği politikaları RAM bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtması amacıyla yapılan varlık ve risk güncellemelerine paralel olarak yılda en az bir defa gözden geçirilirler. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları yeni gerekli eklemeler yapılarak güncellenir. Ayrıca herhangi bir RAM çalışanı Bilgi Güvenliği Politikalarının gelişmesi ve RAM'ın ihtiyaç duyduğu kontrolleri daha iyi yansıtması amacıyla politikaların değiştirilmesi konusunda Bilgi Güvenliği Yönetim Kurulu'na talepte bulunabilir. Yapılan talepler Bilgi Güvenliği Yönetim Kurulu tarafından ele alınır ve değerlendirilir.
Bilgi Güvenliği Politikası ilkeleri, RAM İnsan Kaynaklarının Personel Yönetmeliği Kurallarına paralel uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

4. Denetleme ve Politikalara Uyulması ve Uyulmama Durumlarının Çözümlenmesi

Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derece sorumludur.

Bilgi Güvenliği Yönetim Kurulu başta Bilgi Güvenliği Ana Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur.
Bilgi Güvenliği Politikası ihlalleri, RAM'ın risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda RAM Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğurabilir. 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.

5. Hedefler

RAM Bilgi Güvenliği, RAM'ın 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 RAM çalışanı bu hedeflere katkı sağlamaktan sorumludur.