GALATAPORT İSTANBUL LİMAN İŞLETMECİLİĞİ VE YARITIMLARI A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi güvenliği politikamızın temel ilkeleri aşağıda sıralanmıştır:

Gizlilik: Şirketimizin bilgi varlıkları yalnızca yetkilendirilmiş kişiler tarafından erişilebilir olacaktır. Müşteriler, çalışanlar ve tedarikçilere ait hassas verilerin korunması esastır.

Bütünlük: Tüm bilgiler doğru ve güvenilir olmalıdır. Bilgilerin yetkisiz kişiler tarafından değiştirilmesi, bozulması ya da silinmesi engellenecektir.

Erişilebilirlik: Kritik bilgi ve sistemler, yetkilendirilmiş kişiler tarafından zamanında erişilebilir olmalıdır. Sistem arızaları ve kesintiler minimize edilecektir.

Galataport, şirket amaçları ve değerleri doğrultusunda; bilgi güvenliğini, iş sürekliliğinini sürdürmeyi ve iyileştirmeyi, şirket bünyesinde risklere maruziyeti en aza indirmeyi taahhüt etmektedir.

Bu nedenle aşağıdakilerin sağlanması Galataport'un politikasıdır:

- ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS)'ni, gizlilik, bütünlük ve erişilebilirliğinin korunması için resmi bir sistem uygulamak için bir araç olarak benimsemek
- Bilgi güvenliğini sağlamak amacıyla, şirketin ihtiyaçlarına uygun stratejik planlar geliştirmek, öncelikli alanları belirlemek, ulaşılabilir hedefler koymak ve bu hedeflere ulaşmak için yol haritası belirlemek
- Bilgi güvenliğini sağlarken, kurumun sahip olduğu tüm bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini garanti altına almak, bu unsurları sürekli izleyerek korunmasını sağlamak ve olası tehditlere karşı dayanıklı hale getirmek
- Bilgi güvenliğiyle ilgili ulusal ve uluslararası standartlara, yasal düzenlemelere ve mevcut sözleşmelere tuyum sağlayarak çalışarak, şirketin güvenilirliğini artırmak ve sektördeki itibarı üzerinde pozitif bir etki yaratmak
- Bilgi güvenliği ile ilgili paydaşların beklentilerini doğru bir şekilde anlamak, bu talepleri analiz ederek ilgili tarafların ihtiyaçlarına uygun çözümler geliştirmek
- Bilgi güvenliği risklerini etkili bir biçimde yönetebilmek için potansiyel güvenlik tehditlerini ve mevcut kontrol önlemlerini kapsamlı bir şekilde değerlendirerek, bu tehditlere karşı alınacak önlemleri sistematik bir yaklaşımla belirlemek

- Bilgi güvenliği risklerini, organizasyonun kabul edebileceği seviyelere indirmek ya da tamamen ortadan kaldırmak amacıyla, gelişmiş risk yönetimi teknikleri ve stratejik yaklaşımlar kullanarak, etkin risk yönetimi yaklaşımına destek olmak
- Bilgi güvenliği risklerinin yönetimi ile güvenlik kontrollerinin etkili bir şekilde işleyebilmesi için yetki ve sorumlulukların açıkça tanımlanması, aynı zamanda bu süreçlerin sağlıklı işletilmesi için gerekli kaynakların ayrılmasını sağlamak
- Bilgi güvenliği ihlallerine karşı hazırlıklı olmak adına, gerekli izleme ve müdahale sistemlerini kurarak, olası güvenlik açıklarının tekrar oluşumunu önlemek adına tedbirler almak
- Bilgi güvenliği ile ilgili paydaşların standartlara uyum sağlaması için farkındalık artırıcı çalışmalar yapmak ve yetkin insan kaynağı oluşturmak
- Bilgi güvenliği yönetim sistemi dokümantasyonunu gözden geçirmek ve güncel olarak yürürlükte tutmak
- Bilgi güvenliği yönetim sistemini sürekli iyileştirme ve olgunlaşma çalışmaları yapmak, en iyi uygulamaları entegre etmek
- Bilgi güvenliği alanında sürekli gelişim sağlamak için, organizasyonun bilgi güvenliği uygulamalarını sürekli olarak gözden geçirip iyileştirerek, olgunlaşma sürecini hızlandırmak ve en iyi uygulamaları entegre etmek