BİLGİ GÜVENLİĞİ POLİTİKASI

RMK Marine ve çalışanları olarak, tasarımını ve üretimini yaptığımız askeri, ticari ve gezi amaçlı deniz taşıtları için ilgili iş süreçlerimiz olan, ithalat, ihracat, transit, gümrükleme gibi gümrük ve dış ticaret işlemlerini ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans ve bilgi işlem gibi faaliyetlerine özgü, iş sürekliliğimize ve bilgi varlıklarımıza ve süreçlerimize yönelik riskleri yönetmek amacıyla;

- ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardının gereklerini yerine getirecek şekilde dokümante edilmesi, belgelendirilmesi ve sürekli iyileştirilmesi,

- Bilgi güvenliği ile ilgili yasalar, mevzuatlar ve sözleşmelere uyulması,

- Bilgi güvenliği sisteminin üç ana öğesi olan gizlilik, bütünlük, ve erişebilirlik kurallarına uygun, bilgi varlıklarına ve süreçlerine yönelik risklerin sistematik olarak yönetilmesi ve güvence altına alınması,

- Bilgi güvenliği yetkinliğini ve farkındalığını artırmak amacıyla teknik ve davranışsal eğitimlerin gerçekleştirilmesi,

amacıyla faaliyetlerimizi, uyguladığımız diğer yönetim sistemleri ile birlikte entegre bir şekilde yöneterek, deniz taşıtları sektöründe bilgi güvenliği yöntem ve yönetiminde örnek bir kuruluş olmak için tüm gayretimizle çalışırız.

Üst Yönetim Bilgi Güvenliği Yönetimi Sistemlerinin sürekli olarak iyileştirilmesi için gerekli kaynakları ve işbirliğini sağlayacağını taahhüt eder.

INFORMATION SECURITY POLICY

As RMK Marine and its employees, in order to manage the risks to our business continuity, information assets, and processes related to our business activities such as import, export, transit, customs clearance, and other customs and foreign trade operations, as well as logistics, warehousing, accounting, finance, and information technologies specific to these operations for the design and production of military, commercial, and leisure marine vessels, we are committed to:

- Documenting, certifying, and continuously improving in compliance with the requirements of the ISO 27001 Information Security Management System standard,

- Complying with all laws, regulations, and contractual obligations regarding information security,

- Systematically managing and safeguarding risks to information assets and processes in accordance with the three main principles of information security: confidentiality, integrity, and availability,

- Conducting technical and behavioral training to increase information security competence and awareness.

By managing our activities in an integrated manner with other management systems we implement, we strive with all our efforts to become an exemplary organization in the field of information security practices and management in the marine vessel industry.

The Top Management undertakes to provide the necessary resources and cooperation to ensure the continuous improvement of the Information Security Management Systems.

Dr. Utku ALANÇ
07.04.2025