INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

Redstar Aviation Information Security Management System (ISMS) is dedicated to managing the security of information related to people, infrastructure, software, hardware, user data, organizational data, any third-party information (electronic records, video recordings, images, printed documents, verbal information, etc.), and financial resources. This responsibility is guided by national and international laws, regulations, contracts, standards, and ethical considerations.

In alignment with our mission and vision, we strive to enhance our service quality by ensuring secure, accessible, continuous, and accurate information, thereby achieving internal and external customer satisfaction. Our ISMS focuses on effective risk management, performance measurement of ISMS processes, and regulating relationships with third parties concerning information security.

Accordingly, through our ISMS Policy, we commit to:

- Allocating the necessary resources with the required competence and skills to ensure information security and defining corporate roles and responsibilities,
- Identifying, evaluating, and implementing necessary improvement activities information risks, ensuring effective risk management, and regularly monitoring and reviewing these activities,
- Preventing unauthorized access, use, modification, disclosure, destruction, transfer, and damage to information assets by upholding the core elements of information security: confidentiality, integrity, and availability,
- Raising awareness by providing Information Security Management and KVKK (Personal Data Protection Law) training to all personnel,
- Implementing and continuously improving measures to ensure compliance with the legal requirements of Law No. 6698,
- Ensuring that employees approach information security with awareness and fulfill their duties responsibly, adhering to published policies, procedures, instructions and announcements,
- Regularly reviewing and controlling the accessibility and continuity of the system,

- Defining, operating, and continually improving processes and scenarios for business continuity, emergency, and crisis management,
- Establishing and overseeing the necessary controls for the operation and continuity of the Information Security Management System through related sub-policies, procedures, and instructions,
- Implementing necessary sanctions in case of information security breaches,
- Protecting the security and brand image of the organization.

This policy is crafted in accordance with ISO 9001 standards, ensuring a commitment to quality management and continuous improvement.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI

Redstar Havacılık (RSA) Bilgi Güvenliği Yönetim Sistemi (BGYS), insan, altyapı, yazılım, donanım, kullanıcı verileri, kuruluş verileri, üçüncü şahıslara ait bilgiler (elektronik kayıtlar, video kayıtları, resimler, basılı belgeler, sözlü bilgiler vb.) ve finansal kaynaklarla ilgili bilgilerin güvenliğini yönetmeye adanmıştır. Bu sorumluluk, ulusal ve uluslararası yasa, yönetmelik, sözleşme, standartlar ve etik değerlere dayanmaktadır.

Misyonumuz ve vizyonumuz doğrultusunda, güvenli, erişilebilir, sürekli ve doğru bilgi sağlayarak hizmet kalitemizi artırmayı, böylece iç ve dış müşteri memnuniyetini sağlamayı amaçlıyoruz. BGYS'miz, etkili risk yönetimi, BGYS süreçlerinin performans ölçümü ve bilgi güvenliği ile ilgili üçüncü taraflarla olan ilişkilerin düzenlenmesi üzerine odaklanır.

Bu doğrultuda BGYS Politikamız ile taahhütlerimiz;

- Bilgi güvenliğini sağlamak için gerekli yetkinlik ve becerilere sahip kaynakları tahsis etmek ve kurumsal rol ve sorumlulukları tanımlamak,
- Bilgi risklerini tanımlamak, değerlendirmek ve gerekli iyileştirme faaliyetlerini uygulayarak etkili risk yönetimini sağlamak, bu faaliyetleri düzenli olarak izlemek ve gözden geçirmek,
- Bilgi güvenliğinin temel unsurları olan gizlilik, bütünlük ve erişilebilirliği koruyarak bilgi varlıklarının yetkisiz erişim, kullanım, değiştirme, ifşa etme, yok etme, aktarma ve zarar görmesini önlemek,
- Tüm personele Bilgi Güvenliği Yönetimi ve KVKK (Kişisel Verilerin Korunması Kanunu) eğitimi vererek farkındalığı artırmak,
- 6698 sayılı kanunun yasal gerekliliklerine uyumu sağlamak ve sürekli iyileştirme önlemlerini uygulamak,
- Çalışanların bilgi güvenliğine bilinçli yaklaşım göstermelerini ve görevlerini sorumluluk bilinciyle yerine getirmelerini, yayınlanan politika, prosedür, talimat ve duyurulara azami dikkat göstermelerini sağlamak,
- Sistemin erişilebilirliğini ve devamlılığını düzenli olarak gözden geçirmek ve kontrol etmek,
- İş sürekliliği, acil durum ve kriz yönetimine yönelik süreç ve senaryoları tanımlamak, işletmek ve sürekli iyileştirmek,

- Bilgi Güvenliği Yönetim Sistemi'nin işletilmesi ve sürekliliğinin sağlanması için gerekli kontrollerin tesisini ve gözetimini ilgili alt politikalar, prosedürler ve talimatlar aracılığıyla sağlamak,
- Bilgi güvenliği ihlallerinde gerekli yaptırımları uygulamak,
- Kuruluşun güvenliği ve marka imajını korumak,

Bu politika, ISO 9001 standartlarına uygun olarak hazırlanmış olup, kalite yönetimi ve sürekli iyileştirme taahhüdünü garanti eder.