Redstar
AVIATION

Information Security Management System

Policy

1-2

RSA has established and implemented an Information Security Policy aligned with the organization's purpose, strategic direction, operational activities, aviation safety requirements and information security needs.

The purpose of this Information Security Policy is to protect information, information assets, information systems, technical records, operational data and supporting infrastructure against information security threats and vulnerabilities that may adversely affect aviation safety, operational continuity, regulatory compliance, business objectives, customers, patients, personnel and other interested parties.

RSA recognises that information security is an integral element of aviation safety, operational resilience and business continuity. Information security risks capable of affecting aviation safety shall be identified, assessed, managed and monitored through the Information Security Management System (ISMS).

The Information Security Policy:

- Is established in accordance with the organization's field of activity, operational structure, aviation operations and information security needs.
- Provides a framework for establishing and reviewing information security objectives.
- Includes a commitment to satisfy applicable legal, regulatory, contractual and customer requirements related to information security.
- Supports compliance with ISO/IEC 27001:2022, EASA Part-IS requirements, DGCA-TR regulations, personal data protection requirements and other applicable legislation.
- Includes a commitment to the continual improvement of the Information Security Management System and the enhancement of information security process maturity.
- Defines general principles, processes and controls for appropriately securing information and communication technology systems,
- technical records, operational data and critical information assets.
- Supports the classification of information according to the level of sensitivity of the information used, generated or received from other parties.
- Supports the integration of ISMS requirements into the organization's operational and management processes.
- Supports the protection of confidentiality, integrity, availability, authenticity and continuity of information assets.
- Supports the effective management of information security risks that may impact aviation safety, operational continuity, airworthiness, technical data integrity and critical operational processes.
- Supports the prevention, detection, reporting, investigation, analysis, management and recovery of cybersecurity incidents, information security occurrences and vulnerabilities.
- Supports a "Just Culture" approach encouraging the reporting of vulnerabilities, suspicious activities, anomalies and information security incidents.
- Supports personnel trustworthiness, competence, awareness and accountability regarding information security responsibilities.

- Supports regular training and awareness activities to improve information security awareness throughout the organization.
- Promotes information security responsibilities at all management and operational levels.
- Ensures that all information security activities contribute to the protection and enhancement of aviation safety.

The following Information Security Objectives are established**:**

- Protection of critical information assets and aviation-related information systems;
- Reduction of information security risks to an acceptable level;
- Effective management of information security occurrences, vulnerabilities and incidents;
- Compliance with EASA Part-IS, ISO/IEC 27001 and applicable regulatory requirements;
- Enhancement of information security awareness and competence throughout the organization;
- Continual improvement of the effectiveness and maturity of the Information Security Management System.

This Policy applies to all employees, managers, contracted personnel, temporary personnel, service providers and third parties who access, process, manage or support RSA information assets or information systems.

The Information Security Policy:

- Is established, maintained and controlled as documented information.
- Is communicated within the organization and made accessible to all employees. Is
- made available to interested parties where appropriate.
- Is reviewed at least annually, and whenever necessary due to changes in organizational activities, operational structure, technological infrastructure, regulatory requirements or information security risks, to ensure its continuing suitability, adequacy and effectiveness.

Accountable Manager/CEO
C. Emre DURSUN

Redstar
AVIATION

Bilgi Güvenliği Politikası

1-2

Redstar Havacılık (RSA) kuruluşun amacı, stratejik yönü, operasyonel faaliyetleri, havacılık emniyeti gereklilikleri ve bilgi güvenliği ihtiyaçları ile uyumlu bir Bilgi Güvenliği Politikası oluşturmuş ve yürürlüğe almıştır.

Bu Bilgi Güvenliği Politikasının amacı; bilgi varlıklarının, bilgi sistemlerinin, teknik kayıtların, operasyonel verilerin ve destekleyici altyapıların; havacılık emniyetini, operasyonel sürekliliği, yasal uyumu, kurumsal hedefleri, müşterileri, hastaları, personeli ve diğer ilgili tarafları olumsuz etkileyebilecek bilgi güvenliği tehditleri ve zafiyetlerine karşı korunmasını sağlamaktır.

RSA, bilgi güvenliğini havacılık emniyetinin, operasyonel dayanıklılığın ve iş sürekliliğinin ayrılmaz bir parçası olarak kabul etmektedir. Havacılık emniyetini etkileyebilecek bilgi güvenliği riskleri, Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında belirlenmekte, değerlendirilmekte, yönetilmekte ve izlenmektedir.

Bilgi Güvenliği Politikası;

- Kuruluşun faaliyet alanına, operasyonel yapısına, havacılık faaliyetlerine ve bilgi güvenliği ihtiyaçlarına uygun olarak belirlenmektedir.
- Bilgi güvenliği hedeflerinin oluşturulması ve gözden geçirilmesi için çerçeve sağlamaktadır.
- Bilgi güvenliği ile ilgili uygulanabilir yasal, düzenleyici, sözleşmesel ve müşteri şartlarının yerine getirilmesine yönelik taahhüt içermektedir.
- ISO/IEC 27001:2022 standardı, EASA Part-IS gereklilikleri, SHGM düzenlemeleri, KVKK ve ilgili mevzuat gerekliliklerinin karşılanmasını desteklemektedir.
- Bilgi Güvenliği Yönetim Sistemi'nin sürekli iyileştirilmesine ve bilgi güvenliği süreç olgunluğunun artırılmasına yönelik taahhüt içermektedir.
- Bilgi ve iletişim teknolojileri sistemlerinin, teknik kayıtların, operasyonel verilerin ve kritik bilgi varlıklarının uygun şekilde korunmasına yönelik genel prensipleri, süreçleri ve kontrolleri tanımlamaktadır.
- Kullanılan, üretilen veya üçüncü taraflardan elde edilen bilgilerin hassasiyet seviyelerine göre sınıflandırılmasını desteklemektedir.
- BGYS gerekliliklerinin kuruluş süreçlerine entegre edilmesini desteklemektedir.
- Bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik, doğruluk (authenticity) ve sürekliliğinin korunmasını desteklemektedir.
- Havacılık emniyetini, operasyonel sürekliliği, uçuşa elverişliliği, teknik veri bütünlüğünü ve kritik operasyon süreçlerini etkileyebilecek bilgi güvenliği risklerinin etkin şekilde yönetilmesini desteklemektedir.
- Siber güvenlik olaylarının, bilgi güvenliği olaylarının ve güvenlik açıklarının önlenmesini, tespit edilmesini, raporlanmasını, araştırılmasını, analiz edilmesini, yönetilmesini ve olaylardan kurtarma faaliyetlerinin etkin şekilde yürütülmesini desteklemektedir.
- Güvenlik açıklarının, şüpheli durumların, anomalilerin ve bilgi güvenliği olaylarının raporlanmasını teşvik eden "Adil Kültür (Just Culture)" yaklaşımını desteklemektedir.
- Bilgi güvenliği ile ilgili görevleri bulunan personelin güvenilirlik (trustworthiness), yetkinlik, farkındalık ve hesap verebilirlik ilkelerine uygun şekilde görev yapmasını desteklemektedir.

- Bilgi güvenliği farkındalığının artırılması amacıyla düzenli eğitim ve bilinçlendirme faaliyetlerinin yürütülmesini desteklemektedir.
- Bilgi güvenliği ile ilgili görev, yetki ve sorumlulukların tüm yönetim ve operasyon seviyelerinde sahiplenilmesini desteklemektedir.
- Gerçekleştirilen tüm bilgi güvenliği faaliyetlerinin havacılık emniyetinin korunmasına ve geliştirilmesine katkı sağlamasını hedeflemektedir.

Aşağıdaki Bilgi Güvenliği Hedefleri oluşturulmuştur:

- Kritik bilgi varlıklarının ve havacılık faaliyetleri ile ilişkili bilgi sistemlerinin korunması, Bilgi
- güvenliği risklerinin kabul edilebilir seviyeye indirilmesi,
- Bilgi güvenliği olaylarının, güvenlik açıklarının ve siber olayların etkin şekilde yönetilmesi, EASA
- Part-IS, ISO/IEC 27001 ve uygulanabilir düzenleyici gerekliliklere uyumun sağlanması, Kuruluş
- genelinde bilgi güvenliği farkındalığı ve yetkinliğinin geliştirilmesi,
- Bilgi Güvenliği Yönetim Sistemi'nin etkinliğinin ve olgunluk seviyesinin sürekli iyileştirilmesi.

Bu Politika; RSA bilgi varlıklarına veya bilgi sistemlerine erişen, bunları kullanan, işleyen, yöneten veya destekleyen tüm çalışanlar, yöneticiler, geçici personel, yükleniciler, hizmet sağlayıcılar ve üçüncü taraflar için geçerlidir.

Bilgi Güvenliği Politikası;

- Dokümante edilmiş bilgi olarak oluşturulmakta, sürdürülmekte ve kontrol edilmektedir.
- Kuruluş içerisinde tüm çalışanlara duyurulmakta ve erişilebilir durumda tutulmaktadır.
- Uygun olması durumunda ilgili tarafların erişimine sunulmaktadır.
- Sürekli uygunluğunun, yeterliliğinin ve etkinliğinin sağlanması amacıyla en az yılda bir kez ve ayrıca kuruluş faaliyetlerinde, operasyonel yapısında, teknoloji altyapısında, düzenleyici gerekliliklerde veya bilgi güvenliği risklerinde önemli değişiklikler olması durumunda gözden geçirilmekte ve gerekli görüldüğünde güncellenmektedir.

Sorumlu Müdür/CEO

C. Emre DURSUN