



**Supplier & Service  
Provider Information  
Security Management  
Policy**

▶ 1-2

Redstar Aviation (RSA) is committed to managing its relationships with suppliers, service providers, business partners and other third parties involved in the delivery of its activities by taking into account information security, operational continuity, aviation safety and applicable legal, regulatory and contractual requirements.

The purpose of this Policy is to ensure that information security risks arising from third parties that access RSA information assets, systems, data or facilities, or provide services on behalf of RSA, are appropriately managed and that necessary security requirements are applied throughout the supplier relationship lifecycle.

RSA recognizes that information security in supplier and service provider relationships shall be managed not only at the contracting stage, but throughout the entire lifecycle of the relationship, including selection, assessment, service delivery, change and termination.

Within this framework, RSA:

- Evaluates and classifies suppliers and service providers using a risk-based approach, considering the criticality of the services provided, access to information and systems, sensitivity of the data processed and potential impact on operations.
- Ensures that security requirements appropriate to the identified level of risk are established and applied for critical suppliers and those considered significant from an information security perspective.
- Supports the assessment of service scope, information security capabilities, business continuity arrangements, data processing conditions, use of subcontractors and other relevant security considerations during supplier selection and pre-assessment activities.
- Ensures that information security risks arising from supplier relationships are identified, assessed and monitored within the ISMS risk management processes and that appropriate risk treatment activities are implemented where necessary.
- Ensures that supplier and service provider agreements appropriately address, according to the nature and risk level of the service, requirements relating to confidentiality, information classification, access control, incident and breach notification, service levels, business continuity, backup, data security, encryption, subcontractor management, audit rights and service termination.
- Requires third-party access to RSA information assets and systems to be limited to business needs, appropriately authorized, controlled and traceable where necessary.
- Supports the monitoring and evaluation of supplier performance, service-level commitments and compliance with applicable information security requirements at a frequency and level appropriate to the associated risk.
- Ensures that information security incidents and suspected breaches originating from suppliers or service providers are reported, assessed and managed in accordance with RSA information security incident management processes.
- Ensures that changes to supplier services that may affect RSA information security, operational continuity or critical processes are evaluated and, where necessary, incorporated into applicable risk and change management processes.



- Requires the evaluation of data location, data transfer, access security, service continuity, use of subcontractors and other applicable information security requirements in relation to cloud services and third-party information systems.
- Supports the assessment of risks arising from subcontractor relationships that may affect RSA information assets and services and the application of relevant security requirements to such parties where appropriate.
- Requires that, upon termination of a service relationship or change of supplier, appropriate measures are taken for the return of RSA information and assets, termination of third-party access, secure deletion or disposal of data where applicable, and preservation of operational continuity for critical services.
- Evaluates continuity risks arising from supplier dependency in critical services and supports the establishment of alternative service, transition or business continuity arrangements where necessary.
- Ensures that applicable legal, regulatory, contractual, personal data protection and customer requirements are considered and addressed in supplier and service provider relationships.
- Ensures that non-conformities, security weaknesses or control deficiencies identified in supplier management activities are addressed through applicable corrective and improvement processes.
- Ensures that where exceptions to the requirements of this Policy are necessary, such exceptions are assessed on a risk basis, approved by authorized personnel, supported by appropriate compensating controls and documented.

RSA recognizes that the secure and effective management of supplier and service provider relationships is an important element in protecting information security, operational resilience, business continuity and aviation safety.

This Policy applies to all suppliers, service providers, consultants, outsourced personnel, business partners, subcontractors and other relevant third parties that provide services to RSA, access RSA information assets, information systems, data or facilities, or process information on behalf of RSA.

The Policy is implemented taking into account the information security requirements of ISO/ IEC 27001:2022 relating to supplier relationships, supplier agreements, monitoring and change management of supplier services, and the use of cloud services.

The Supplier and Service Provider Information Security Management Policy:

- Is established, maintained and controlled as documented information.
- Is communicated to relevant personnel within the organization and made accessible as appropriate.
- Is made available, where appropriate, to suppliers, service providers and other interested parties.
- Is reviewed at least annually and whenever significant changes occur in the supplier environment, service models, technological infrastructure, legal or regulatory requirements, or information security risks, and is updated where necessary.

**Accountable Manager/CEO**

