Cybersecurity Standards for SITA Suppliers

Enterprise Information Security

Office - EISO

17th March 2026

1. Introduction

SITA promotes a secure and resilient ecosystem across its global supplier and service-partner network. This Standard summarizes SITA's minimum-security expectations for any third party that handles, accesses, or can influence SITA information, systems, networks, customer data, or personal data.

2. Purpose

This Supplier Security Standard (the "Standard") defines minimum information security requirements for suppliers, vendors, partners, contractors, and other third parties ("Suppliers") that provide products or services to SITA involving access to Company information, Company systems/networks, customer data, personal data, or other confidential/sensitive information.

This Standard supports the protection of information assets and helps ensure compliance with applicable laws, regulations, and contractual obligations.

This Standard applies to supplier engagements including outsourcing, managed services, cloud services (SaaS/PaaS/IaaS), software development, and hardware procurement—across on-premises and cloud environments where supplier systems interface with SITA networks or data.

- All suppliers that access, process, transmit, store, or manage SITA data or connect to SITA networks.
- All supplier systems/services that can affect the confidentiality, integrity, or availability of SITA information.
- All delivery locations/environments (on-premises or cloud) used to provide services to SITA.

3. Requirements

Suppliers are expected to implement security practices aligned with this Standard and be able to demonstrate their security posture upon request. Minimum requirements include:

- **Security governance:** Assign security responsibility and maintain an information security management process appropriate to the organization.
- **Data protection:** Protect data from unauthorized access/alteration/destruction; classify by sensitivity; encrypt sensitive data in transit and at rest using industry-accepted standards; securely return or delete SITA/Company data at contract end.
- **Incident management:** Detect, respond, contain, remediate, perform root-cause analysis; notify SITA without undue delay of any security breach or suspected compromise impacting SITA data/services.
- **Access control:** Strong authentication/authorization; least privilege and segregation of duties; periodic access reviews; rapid deprovisioning; restrict and monitor privileged access.
- **Confidentiality:** Use NDAs where appropriate for personnel with access to SITA information resources.

- **Risk management:** Identify, assess, and treat risks; review periodically and when services/systems change.
- **Secure development & change:** Follow secure development practices; separate dev/test/prod (where applicable); assess security impact prior to implementation; remediate vulnerabilities in a timely manner.
- **Vulnerability & patch management:** Identify vulnerabilities; apply patches within a risk-based timeframe; use scanning or equivalent mechanisms where appropriate.
- **Personnel security:** Background checks where legally permissible/appropriate; security awareness training; confidentiality obligations.
- **Physical security:** Protect facilities, systems, and media containing Company data; control physical access to sensitive areas.
- **Logging & monitoring:** Log security-relevant events; protect logs; monitor for suspicious/unauthorized activity.
- **Business continuity:** Maintain and regularly test business continuity/disaster recovery plans; define appropriate availability and recovery objectives.
- **Security policies:** Management-approved, communicated to relevant parties, and reviewed at least annually.
- **Non-Disclosure Agreements (NDAs):** Where appropriate, ensure personnel who perform work for (or have access to) SITA information resources are covered by duly executed confidentiality/non-disclosure obligations.

4. Use of Subcontractors

Suppliers must:

- Obtain required approval before engaging subcontractors that will access SITA data or connect to SITA systems.
- Flow down requirements equivalent to this Standard and verify subcontractor compliance.
- Remain fully responsible for subcontractor performance and security obligations.

5. Compliance and Assurance

Suppliers may be required to demonstrate compliance through one or more of the following:

- Provide evidence on request (e.g., security questionnaires, policy excerpts, or attestations).
- Provide independent assurance where applicable (e.g., ISO 27001 certificate, SOC 2 Type II report, or equivalent).
- Support remediation plans and timelines for identified gaps.

6. Right to Audit

SITA reserves the right, subject to contractual terms, to:

- Assess supplier compliance (including via questionnaires, evidence review, or onsite/remote audits).
- Request remediation for identified deficiencies within agreed timelines.
- Engage a qualified third party to perform audits where contractually permitted.

7. Exceptions

Any exception to this Standard must:

- Be documented, risk-assessed, and time-bound.
- Be approved by SITA (and/or the contract owner) before implementation.
- Include compensating controls and a remediation plan where applicable.

8. Non-compliance

Failure to comply with this Standard may result in:

- Required corrective actions and increased oversight.
- Service restrictions, suspension, or termination consistent with contractual terms.
- Other remedies available to SITA under the contract or applicable law.

9. Offboarding

Suppliers must:

- Return or securely delete SITA/Company data (including backups) as instructed and within agreed timelines.
- Revoke access (accounts, keys, tokens) and confirm deprovisioning is complete.
- Support transition activities and provide relevant security evidence/records on request.

10. Review and Updates

This Standard may be updated to reflect:

- Changes to laws, regulations, or contractual requirements
- Changes to SITA security policies/standards and risk posture
- New or emerging threats and security best practices
- Suppliers are responsible for complying with the latest published version.

11. Contact

For questions about this Standard, contact:
Email: supplier.security@sita.aero
Department: Enterprise Information Security Office / Third Party Risk Management