Security Technical and Operational Measures (TOMs)

Global SITA security measures

This applies to relevant SITA group services under applicable signed customer agreements, if referred to in part 3.1 of the relevant Security Technical and Organizational Measures (TOM) Appendix or if referenced at this link by any other applicable agreement.

The below security measures are implemented at a global level in SITA:

a) Information security governance

The SITA Executive Leadership Team (ELT) led by SITA's CEO has executive responsibilities for governance matters within SITA, including of the management of Information Security risks.

SITA has a set of enterprise level Information Security policies and standards defined with the objective of specifying and communicating security requirements to ensure the safeguarding of SITA information assets and the provision of a safe and secure computing environment based on the most current information security risks.

The policies and standards are aligned to industry security practice and aim at covering all the security sub-domains per ISO 27001/2 standards. SITA enterprise security policies are reviewed on an annual basis.

References	
Related ISO/IEC 27002:2022 controls	05.01. Policies for information security; 05.02. Information security roles and responsibilities; 05.04. Management responsibilities;
Related GDPR principles	Accountability

b) Human resources security

SITA has defined a "Security in Human Resources Standard", established for the protection of information, and information processing facilities, as applicable to Human Resources (HR) processes and practices. This standard sets requirements on the following topics: background checks, on-boarding training, managers' responsibilities for security, cautious termination process, on-going information security requirements, notification of a termination or long-term leave and account suspension.

All SITA employees are encouraged to undertake regular "Security Awareness" trainings. In addition, SITA developers are trained by our CISO team on cybersecurity industry practices.

A mandatory "Information Security Essentials" course is integrated into SITA's induction program and new hires are required to complete the course within the first 60 days of employment.

References	
Related ISO/IEC 27002:2022 controls	06.01. Screening; 06.02. Terms and conditions of employment; 06.03. Information security awareness, education and training;
Related GDPR principles	Lawfulness, fairness and transparency

c) Security in third party relationships

SITA has defined a "Third Party Service Delivery Management Standard", establishing requirements while dealing with third parties/suppliers and establishing the Information Security related processes required throughout the complete vendor management lifecycle. This standard sets requirements for the following topics: Information Security responsibilities, segregation of duties, non-disclosure agreements, audit clause, subcontracting, user management and certifications.

References	
Related ISO/IEC 27002:2022 controls	05.19. Information security in supplier relationships; 05.20. Addressing information security within supplier agreements; 05.22. Monitoring, review and change management of supplier services;
Related GDPR principles	Accountability

d) Physical security

SITA has defined a “Physical & Environmental Security Standard”, establishing requirements to maintain confidentiality, integrity and availability of information assets from physical and environmental threats. This standard sets requirements on the following topics: physical access management, identifying staff and visitors, security perimeters, using Electronic Access Cards (EAC) and environmental threats.

SITA risk assessments are also covering physical security controls.

References	
Related ISO/IEC 27002:2022 controls	07.01. Physical security perimeters; 07.03. Securing offices, rooms and facilities; 07.04. Physical security monitoring
Related GDPR principles	Integrity and confidentiality (security)

e) Asset management

SITA has defined an “Asset Management & Media Handling Standard”, establishing requirements regarding asset inventory, security classification, ownership, and secure media handling. This standard sets requirements on the following topics: inventorying assets, classification of assets, assigning ownership to assets and returning assets.

References	
Related ISO/IEC 27002:2022 controls	05.09. Inventory of information and other associated assets; 05.10. Acceptable use of information and other associated assets; 05.11. Return of assets
Related GDPR principles	Integrity and confidentiality (security)

f) Secure development lifecycle

SITA follows a development process consisting of several stages (product creation, maintenance, and evolution) which has been adapted to incorporate Agile DevOps principals. Security governance is an integral part of the assessment, and Information Security approvals apply at the end of each Stage.

SITA’s efforts in embedding security into software development leverage existing processes, standards and techniques, such as the Open Web Application Security Project Software Assurance Maturity Model (OWASP SAMM) and Microsoft’s Secure Development Lifecycle (SDL). SITA's software security practices are regularly benchmarked for compliance and maturity using Software Assurance Maturity Model (SAMM) as a guide.

Each in-development SITA software undergoes source code security testing using static security code review tools and manual peer review. At the end of the development process, SITA software solutions are verified to ensure that security requirements have been identified and the right security controls have been implemented.

All SITA developers and architects are required to attend regular and up-to-date software security training that covers secure coding techniques, common security risks and threat modelling.

References	
Related ISO/IEC 27002:2022 controls	08.25. Secure development life cycle; 08.28. Secure coding; 08.29. Security testing in development and acceptance;
Related GDPR principles	Purpose limitation; Data minimization; Storage limitation

g) Incident management

SITA has defined “Security Incident Response Processes” managed by the SITA Global Services (SGS) Security Practice and Corporate Information Security Office (CISO) including forensic investigation into suspected incidents. SITA Security Incident Response Teams are engaged for priority incidents. This process sets requirements on the following topics: preparation for incident response, identification of a security incident, containment, eradication, recovery and lessons learned.

SITA also subscribes to an “Incident Response Retainer” with an independent external provider to support any incident response activities.

Security incident management generally covers measures and processes implemented to allow the monitoring and detection of security events and the appropriate response to them.

References	
Related ISO/IEC 27002:2022 controls	05.24. Information security incident management planning and preparation; 05.25. Assessment and decision on information security events; 05.26. Response to information security incidents; 05.27. Learning from information security incidents
Related GDPR principles	Integrity and confidentiality (security)

h) Independent information security audit and certifications

SITA’s Command Centers in Singapore and Montreal are ISO 27001 certified.

SITA security professionals also maintain proficiency in their field of expertise and maintain adequate certifications. SITA security professional staff includes GIAC-Certified Forensic Analyst (GCFA) practitioners, GPEN and CEH certifications, ISO 27001 Lead Auditor and ISO 27001 Lead Implementer, CISSP, CIPP/E and CIPM specialists.

References	
Related ISO/IEC 27002:2022 controls	05.35. Independent review of information security; 05.36. Conformance with policies, rules and standards for information security
Related GDPR principles	Integrity and confidentiality (security); Accountability