Security Technical and Organizational Measures (TOMs) Appendix for SITA Flex as a Service

Version: January 2025

APPENDIX 2 FOR ANNEX A OF DATA PROTECTION AGREEMENT

1. Purpose

The Security Measures Appendix's purpose is to list all the technical and organizational measures (TOMs) implemented by SITA to secure any personal data processed as defined in the Data Processing Agreement (DPA) to which this appendix is attached.

The security measures defined in section 3 implement the requirements of Article 32 of the GDPR and its protection objectives in concrete terms.

The detailed measures apply to the Service.

Evidence of the measures implemented and maintained by SITA may be requested by the Customer.

Relevant references to the respective ISO 27002:2022 controls are attached to each of the measures.

2. Definitions and Explanations

2.1. Explanation of GDPR principles (Art. 5)

Lawfulness, fairness, and transparency: the organization must identify valid grounds to process data, handle it in ways that people would reasonably expect and to inform people about their personal data being processed.

Purpose limitation: the organization must be clear about personal data processing purpose and specify it in privacy information for individuals. Valid ground must be obtained (e.g., consent) in case of new purpose.

Data minimization: the organization must ensure the processed personal data is adequate, relevant, and limited to only what is necessary.

Accuracy: the organization must ensure the held personal data is accurate and take responsible steps to correct or erase the data as soon as possible if an inconsistence or error is discovered.

Storage limitation: the organization must not keep personal data for longer than needed and must justify how long is personal data kept, with clear retention periods. Held personal data should be reviewed, erased, or anonymized when no longer needed.

Integrity and confidentiality (security): the organization must ensure to have appropriate security measures in place to protect the held personal data.

Accountability: the organization must take responsibility for what it does with personal data and how it complies with other principles. Measures and records should be available to demonstrate compliance.

2.2. Definitions specific to this Appendix:

API: means Application Programming Interface that enables data transmission between one software product and another.

CAB: means Change Advisory Board which is the managerial instance supporting the assessment, prioritization, authorization, and scheduling of changes.

CCTV: means Closed-Circuit Television which is also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

CI/CD: means Continuous Integration and Continuous Development which is a modern software development practice in which incremental code changes are made frequently and reliably. Automated build-and-test steps triggered by CI ensure that code changes being merged into the repository are reliable. The code is then delivered

quickly and seamlessly as a part of the CD process. The CI/CD pipeline refers to the automation that enables incremental code changes from developers' desktops to be delivered quickly and reliably to production.

ITSM: means IT Service Management tool which is a software solution that helps organizations manage the lifecycle of IT services: provision, tracking changes, managing incidents and requests.

MFA: means Multi-Factor Authentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource.

Oauth2: means Open Authorization widely used standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user

Personal data: means any information relating to a natural person identified or who can be identified, directly or indirectly, by reference to an identification number or to one or more elements specific to him/her.

RBAC: means Role Based Access Control used as a model to handle security and permissions in which roles and permissions are assigned within an organization's IT infrastructure and applications. Access permissions are assigned based on a defined role model. Defined user roles represent a set of work processes within the organization.

SAST, DAST and/or SCA: means a secure code review, being a specialized task involving manual and/or automated review of an application's source code to identify security-related vulnerabilities. Static Application Security Testing (SAST) aims at identifying common flaws before compiling a release. Dynamic Application Security Testing (DAST) aims at examining a running build and detect issues such as misconfiguration and error handling. Software Composition Analysis (SCA) is an automated process that identifies vulnerabilities in software libraries and open-source components licenses in a codebase. This analysis is performed to evaluate security, license compliance, and code quality.

SoD: means Segregation of Duties which is the concept of having more than one person required to complete a task. It is an administrative control used by organizations to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

Service: means SITA Flex as a Service

SIEM: means Security Information and Event Management which supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of logs, allowing to raise alerts based on security events.

Transport Layer Security (TLS): means a cryptographic protocol that provides end-to-end security of data sent between applications over a network.

TDE: means Transparent Data Encryption serves as a security mechanism that encrypts data at the storage layer, protecting sensitive data contained in database files on disk.

3. Security Technical and Operational Measures (TOMs)

3.1. Global SITA security measures

SITA has implemented security measures that apply to the organization as a whole, and hence to all of SITA's products and services.

Please refer to the following link to have access to these global security measures:

https://www.sita.aero/globalassets/docs/other/Global-Security-TOMs.pdf

This link may be updated periodically by SITA, but it shall not be amended in such a way that causes material decrease in security measures applied by SITA under this TOM.

3.2. SITA Flex as a Service specific security measures

The below security measures are implemented specifically for SITA Flex as a Service:

3.2.1. Network security

The below specific network security measures are implemented for the Service:

- Network authorization provided using Oauth2
- API gateway

References	
Related ISO/IEC 27002:2022 controls	08.20. Networks security; 08.21. Security of network services; 08.22. Segregation of networks
Related GDPR principles	Integrity and confidentiality (security)

3.2.2. Operational security

The below specific operational security measures are implemented for the Service:

- Vulnerability management (vulnerability management policy, process and procedure, vulnerability scanning, penetration testing)
- Change management (change management policy, process and procedure, use of an ITSM tool, change advisory board (CAB))
- System operating procedures
- Logging and monitoring (product logs collection and protection, manual logs analysis, automated logs analysis through a SIEM for system security monitoring)

  SITA Flex as a Service is built on Platform as a Service deployed in Azure.

References	
Related ISO/IEC 27002:2022 controls	05.37. Documented operating procedures; 08.06. Capacity management; 08.07. Protection against malware; 08.08. Management of technical vulnerabilities; 08.15. Logging; 08.16. Monitoring activities; 08.32. Change management
Related GDPR principles	Integrity and confidentiality (security)

3.2.3. Information protection

The below specific information protection security measures are implemented for the Service:

- Secured information exchange / data in transit encryption (through secured and accepted protocols (TLS 1.2) and industry standard encryption mechanisms (TDE)

- Passenger personal data and other data (including data contained in logs) is not stored by the Service, it is deleted immediately when the session ends
- Logging of data processing is disabled by default to avoid retention of any personal data

References	
Related ISO/IEC 27002:2022 controls	05.12. Classification of information; 05.13. Labelling of information; 05.14. Information transfer; 08.10. Information deletion; 08.11. Data masking; 08.12. Data leakage prevention; 08.24. Use of cryptography
Related GDPR principles	Data minimization; Accuracy; Storage limitation; Integrity and confidentiality (security)

3.2.4. Access control and authentication

The below specific access control and authentication security measures are implemented for the Service:

- Strong authentication for APIs & SITA Privileged Users using Identity Management (password policy, enforcement of password complexity rules, account sessions management with account locker, log out time)
- MFA for SITA privileged users
- Protection of authentication information (personal passwords generated automatically at enrolment with by default password to be changed, secure transmission of by default authentication information to users, authentication information encryption)
- Restricted access to source code (role-based access, fine-grained permissions management, regular permissions review)
- Segregation of duties for SITA Privileged Users accessing the system remotely (SoD) (SoD policy, process and procedure, SoD matrix, account creation and access rights validation process ensuring SoD)

References	
Related ISO/IEC 27002:2022 controls	05.15. Access control; 05.17. Authentication information; 05.18. Access rights; 08.02. Privileged access rights; 08.03. Information access restriction; 08.04. Access to source code; 08.05. Secure authentication
Related GDPR principles	Integrity and confidentiality (security)

3.2.5. Application security

The below specific application security measures are implemented for the Service:

- Secure coding (secure coding policy, process and procedure, Secure Software Development Lifecycle management, automated SAST, DAST)
- Vulnerability scanning (regular exposed assets vulnerability scanning)
- Penetration testing (regular exposed assets penetration testing)
- Secure CI/CD platform

References	
Related ISO/IEC 27002:2022 controls	08.26. Application security requirements; 08.27. Secure system architecture and engineering principles

Related GDPR principles	Purpose limitation; Data minimization; Storage limitation

3.2.6. Service resilience

The below specific service resilience security measures are implemented for the Service:

- Configuration data resilience is managed through redundant design: No data is backed up.
- Systems redundancy to meet SLAs
- Crisis management (crisis management policy, process and procedure, crisis management tooling (e.g., ad hoc communication paths, reflex cards, emergency button))

References	
Related ISO/IEC 27002:2022 controls	08.13. Information backup; 08.14. Redundancy of information processing facilities
Related GDPR principles	Storage limitation; Integrity and confidentiality (security);

3.2.7. Cloud security

The below specific cloud security measures are implemented for the Service by the SITA cloud provider:

- Data Center access restriction (cloud security policy, Data Center physical access monitoring, badging system, badging systems logs collection and review, CCTV)
- Cloud redundancy capabilities (hardware redundancy, geographic redundancy)
- Cloud backup recovery testing

References	
Related ISO/IEC 27002:2022 controls	05.23 Information security for use of cloud services; 08.14 Redundancy of information processing activities;
Related GDPR principles	Integrity and confidentiality (security)