Security Technical and Organizational Measures (TOM) Appendix for SITA TransitVision service schedule

Version: June 2022

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 (TOM) 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:

AD: means Active Directory which is a Microsoft directory service used for the management of identities' permissions and network access.

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

CWE: means Common Weakness Enumeration which is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

DevOps: means a set of practices that combines software development (Dev) and IT operations (Ops). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.

DPA: means Data Processing Agreement which is a legally binding contract that states the rights and obligations of each party concerning the protection of personal data.

GDPR: means General Data Protection Regulation which is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

HTTPS: means Hypertext Transfer Protocol Secure which is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and a website.

IP: means Internet Protocol which is the principal communications protocol in the IETF Internet protocol suite for specifying system address information when relaying datagrams across network boundaries.

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

LDAP: means Lightweight Directory Access Protocol which is an open and cross platform protocol used for directory services authentication. LDAP provides the communication language that applications use to communicate with other directory services servers.

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

NTP: means Network Time Protocol which is an internet protocol used to synchronize with computer clock time sources in a network.

OEM: means Original Equipment Manufacturer which refers to a company that builds a product designed for end-users. OEM licenses are linked to the purchase of hardware, such as the pre-installed OS versions for new laptops.

OS: means Operating System which is a program that runs on a computer and provides a software platform on which other programs can run.

OWASP Top 10: means Open Web Application Security Project Top 10 vulnerability report, which is a regularly updated report outlining security concerns for web application security, focusing on the 10 most critical risks observed in the industry at the moment of release.

RBAC: means Role Based Access Control model which is an approach to handling 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 tools for 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.

Service: means SITA Information Display System.

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.

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 organisations to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

TOMs: means Technical and Organizational Measures which is a Data Privacy annex listing security controls aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

VPN: means Virtual Private Network which provides a secure, often encrypted connection between two private networks over a public network. A site-to-site VPN is designed to securely connect two geographically distributed sites. A remote access VPN is designed to link remote users securely to a corporate network.

3. Security Technical and Organizational Measures (TOM)

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 TransitVision specific security measures

The below security measures are implemented at SITA TransitVision service level:

3.2.1. Network security

The below specific network security measures are implemented for the Service. The service consists of: (a)SITA TransitVision (on-premises – SITA managed) and (b) SITA TransitVision (on-premises – Customer managed) option. This schedule applies to the relevant option selected by the Customer, as appliable.

SITA TransitVision (on-premises – SITA managed):

- Firewall: server-based firewalls are implemented both for internal traffic and external traffic filtering,
- Access to network: SITA VPN with MFA is implemented for managed sites with remote connection secured through a jump server, available to SITA teams for support purpose,
- Network authentication: network authentication relies on Active Directory using LDAP protocol.

SITA TransitVision (on-premises – Customer managed):

- Network security falls under the Customer's responsibility. Should Customer provide an external access to their network for SITA support purpose, the security measures implemented in that case are not under SITA's responsibility but should follow SITA's recommendations.

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

3.2.2. Operational security

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

SITA TransitVision (on-premises – SITA managed):

- Antivirus: antivirus agents are deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
  - Vulnerability scans are performed by SITA on a bi-annual basis,
- Patch management: a patch management process is documented and implemented:
  - A dedicated team is in place and relies on industrialized patching tools; security patches are tested and certified in a test environment before being deployed in production,
- Change management: a change management procedure is documented and implemented:
  - An ITSM tool is used to track all changes; all non-standard changes go through the CAB process,
- System operating procedures: standard operating procedures are documented,

- Logging and monitoring:
    - Both user activities in the application and infrastructure events are logged,
    - NTP is in place for clock synchronization,
    - The retention time is set to 30 days by default for both application and infrastructure logs; Customer can modify the retention time up to the limit of the data base storage; Logs purging is automatically performed through a dedicated script as soon as the data retention period is reached. A job is launched on a daily basis and purges all the logs that expired,
    - Active Directory authentication infrastructure logs are sent to SITA SIEM,
- System hardening: a system hardening policy and checklist is documented and implemented:
    - The Windows versions installed are OEM images built by SITA with disabled features to focus on core functions necessary for the application to run.

SITA TransitVision (on-premises – Customer managed):

- Patch management / change management: application patch and change management follows SITA standard documented processes and procedures:
    - An ITSM tool is used to track all application changes and patches, which all go through the CAB process, except for standard changes,
    - System patch management remains under Customer's responsibility,
- Application logging and monitoring: user activities in the application are logged. However, the analysis and storage of these logs remain under Customer's responsibility.
- Antivirus, vulnerability management, capacity management, infrastructure logging and monitoring, system hardening, system operating procedures: these security measures fall under Customer's responsibility but should follow SITA's recommendations.

References	
Related ISO/IEC 27002:2022 controls	05.37. Documented operating procedures; 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:

SITA TransitVision (on-premises – SITA managed):

- Data at rest encryption: databases are encrypted, [NOT APPLICABLE UNLESS SPECIFICALLY REQUESTED AND AGREED AS PART OF THE CONTRACT]
- Data in transit encryption / secure information exchange: personal data communication is encrypted using HTTPS,
- Information deletion: a data retention policy is documented and implemented:
    - The retention time is set to 14 days by default,
    - Customer can modify the retention time up to the limit of the data base storage,
    - SITA shall delete all data without further notice to Customer within 10 days following the end of the configured data retention period,
    - An automatic and daily purge using dedicated jobs is launched as soon as the data retention period has passed.

SITA TransitVision (on-premises – Customer managed):

Information protection security measures fall under Customer's responsibility but should follow SITA's recommendations.

References	
Related ISO/IEC 27002:2022 controls	08.10. Information deletion; 08.24. Use of cryptography
Related GDPR principles	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:

SITA TransitVision (on-premises – SITA managed):

- Authentication: SITA password policy, and timeout and idle-time session management are implemented by default, but it remains configurable by the Customer,
- Multi-factor authentication: an MFA is implemented for VPN authentication,
- Single Sign-On: a Customer SSO service is implemented [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE SSO SERVICE],
- Protection of authentication information: passwords are stored encrypted,
- Restricted access to source code: restricted access to source code is performed based on RBAC model and least privilege; only DevOps teams have access to source code.

SITA TransitVision (on-premises – Customer managed):

- Restricted access to source code: restricted access to source code is performed based on RBAC model and least privilege; only DevOps teams have access to source code,
- Authentication, conditional access, Single Sign On (SSO), protection of authentication information, Segregation of Duties (SoD):
    - These security measures fall under Customer's responsibility but should follow SITA's recommendations.
    - Should Customer provide an external access to their network for SITA support purpose, the access control and authentication security measures implemented in that case are not under SITA's responsibility.

References	
Related ISO/IEC 27002:2022 controls	05.15. Access control; 05.17. Authentication information; 05.18. 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:

SITA TransitVision (on-premises – SITA managed):

- Secure coding: a secure coding policy is documented and implemented:
    - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices.

SITA TransitVision (on-premises – Customer managed):

- Secure coding: a secure coding policy is documented and implemented:
    - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against

vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices.

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:

SITA Transit Vision (on-premises – SITA managed):

- Data backup: a data backup policy is documented and implemented:
  - Database are backed up through daily full backup,
  - The data backup retention time is 14 days by default,
  - SITA shall delete all data backup without further notice to Customer within 10 days following the end of the configured data retention period,
  - Data purging is automatically performed through a dedicated script as soon as the data backup retention period is reached. A job is launched on a daily basis and purges all the backups that expired,
- Systems redundancy:
  - An active/passive failover is activated to switch to a live instance in case of failure of the first one [NOT APPLICABLE IF THE CUSTOMER DOES NOT ACTIVATE FAILOVER],
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

SITA TransitVision (on-premises – Customer managed):

Service resilience security measures fall under Customer's responsibility but should follow SITA's recommendations.

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)