Security Technical and Organizational Measures (TOM) Appendix for SITA Bag Radar Service Schedule

Version: October 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 EU General Data Protection Regulation (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:

CI/CD: means Continuous Integration and Continuous Delivery 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.

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.

Encryption: means a computing process that encodes plaintext/cleartext (unencrypted, human-readable data) into ciphertext (encrypted data) that is accessible only by authorized users with the right cryptographic key.

FDE: means Full Disk Encryption is a technology to protect information by encrypting all data on disk at rest, including temporary, files, programs, and system files.

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.

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.

SSL: means Secure Socket Layer which is a security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

OWASP Top 10: means Open Web Application Security Project Top 10 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.

SITA Privileged Users: means individuals within SITA who are granted elevated access rights to critical systems, infrastructure, or sensitive data.

OAuth 2.0: means Open Authorization 2.0 which is a widely adopted standard that enables applications to access resources on behalf of a user without exposing their credentials. It replaced OAuth 1.0.

RTO: means Recovery Time Objective which is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs.

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 Bag Radar service.

SFTP: means SSH File Transfer Protocol which is a secure file transfer protocol that uses secure shell encryption to provide a high level of security for sending and receiving file transfers.

DevOps: means a modern software development approach that emphasizes collaboration between development (Dev) and operations (Ops) teams.

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.

SSE: means Server-Side Encryption which is a method used by cloud service providers to protect data at rest (i.e., data stored on disk) by automatically encrypting it on the server side before saving it.

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

TACACS+: means Terminal Access Controller Access-Control System Plus which is a security protocol handling remote authentication and related services for network access control through a centralized server.

TDE: means Transparent Data Encryption which is a technology used to encrypt database files at the file level, ensuring that data at rest is protected.

Microsoft Entra ID: means Microsoft's cloud-based identity and access management service.

VLAN: means Virtual Local Area Network which is a broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN.

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 Operational Measures (TOM)

3.1. Global SITA security measures

SITA has implemented security measures that apply to the organization, 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 document.

3.2. SITA Bag Radar specific security measures

The below security measures are implemented at SITA Bag Radar level.

3.2.1 Network security

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

- Network segmentation: Network segmentation is implemented.
  - Each product service (admin, monitoring, core services) is segmented in a VLAN subnet with a firewall in front.
  - Tenant service is run on a specific Azure cloud environment.
- Firewalls:
  - Traffic firewall between platform ingress & egress points and the remote hosts.
  - Web Application Firewalls for traffic between the customer applications and platform ingress point.
- VPN: for remote support teams connecting to the Cloud environment, using SITA MFA.
- Network authentication using protocols such as: Microsoft Entra ID.

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 process is in place to remediate vulnerabilities. Scans are performed monthly.

- The security team receives vulnerability notifications from the vendors and a report with the list of patches to be applied; all vulnerabilities are assessed and can trigger software upgrades.
- Patch management: patch management policy, process and procedure:

  Patches are made available by the vendors and are systematically tested before implementation in production.
- Change management:
  - SITA has a formal change management process in place which requires identification and recording of significant changes alongside an assessment of risk and potential effect of such changes, approval of proposed changes and testing of changes to verify operational functionality of the product/service and underlying Cloud infrastructure.
- Capacity management:
  - Capacity of the Cloud is gathered and analysed to ensure product/service applications meet current and future consumption demands.
- Logging and monitoring: product logs collection and protection, log analysis through a SIEM for system security monitoring.
  - Logs are retained for 3 months.
  - Product/Service and underlying Cloud infrastructure is monitored by security personnel on a 24/7 basis for unauthorized changes and take the appropriate actions to remediate using defined playbooks.
- System hardening: system hardening policy, process and procedure, hardening at asset installation, regular application of hardening baseline
  - The platform hardening is performed by the cloud supplier.
  - Configuration management is performed by Operational team based on approved scanned images.

References	
Related ISO/IEC 27002:2022 controls	05.37. Documented operating procedures; 08.06. Capacity management; 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:

- Data at rest encryption:
  - Data at rest within the Cloud is encrypted with Service Side Encryption (SSE).
  - Product can implement Transparent Data Encryption (TDE) or Full Disk Encryption (FDE) for sensitive data at database and/or disk level.
- Data in transit encryption / secure information exchange: personal data communication is encrypted using HTTPS/SFTP (TLS 1.2 or above).
- Information deletion: a data retention policy is documented and implemented:
  - Information deletion is governed by the SITA Global Data Retention Policy.
  - Login credentials are stored in DB and managed according to account management policies.

- Data minimization:
    - SITA's Global Privacy Policy and SITA's Data Retention Policy require us to retain personal data for no longer than is necessary for the purposes for which it is processed.
    - Personal data is only stored when needed and reduced to the strict scope of processing.

References	
Related ISO/IEC 27002:2022 controls	05.12. Classification of information; 05.14. Information transfer; 08.10. Information deletion; 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:

- Authentication: strong password policy, enforcement of password complexity rules, account sessions management with account locker, logout time.
    - SITA IT Corporate policy is in place for SITA Privileged Users.
    - A multi-factor authentication (MFA) is implemented for administration connection with the VPN.
- API Access management:
    - OAuth 2.0 token-based authentication.
- Protection of authentication information: all passwords are stored encrypted.
    - Secure software is used to manage the credentials, keys and passwords. A second level of authentication is needed to access it.
- Restricted access to source code: A role-based access control policy is implemented, with regular review.

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:

- Security review and architecture review are made.
- Secure coding: a secure coding policy is documented and implemented:
    - It is shared by SITA information security team and followed by developers; a secure coding checklist is used including scans,
    - A DevOps guide is provided to the developers and describes a list of best practices regarding secure coding, data protection and security development measures.
    - SAST, DAST and/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25) including open-source libraries.
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle, before each code release,

- Secure CI/CD platform: Pipelines are used, with restricted permissions on who can run the pipeline and promote the code; deployment requires an approval process,

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:

- Crisis management: SITA has an Issues & Crisis Management Policy; additionally, SITA has an Incident Management Procedure.

References	
Related ISO/IEC 27002:2022 controls	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:

- Datacenter access restrictions: standard Microsoft Azure security measures are implemented by our cloud provider.
- The Service is running on Azure Cloud and rely on Microsoft security.

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)