Security Technical and Organizational Measures (TOM) Appendix for SITA WorldTracer® Bag Mate Service Schedule

Version: September 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:

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.

CIS benchmarks hardening guidelines: mean Center for Internet Security benchmarks hardening guidelines which are also called "CIS benchmarks", are recognized as security state-of-the-art measures for defending IT systems and data against cyberattacks and offer prescriptive guidance for establishing a secure baseline configuration.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

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.

AES: means Advanced Encryption which is a Standard widely used symmetric encryption algorithm that secures data by converting it into unreadable ciphertext and then decrypting it back using the same key.

Oauth2: means Open Authorization 2.0 which is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user. It replaced OAuth 1.0.

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.

Log(s): means records of events or activities generated by software applications, systems, or devices. They provide detailed information about what happened, when it happened, and often why it happened.

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.

IDS: means Intrusion Detection System which is a device or software application that monitors a network or systems for malicious activity or policy violations.

IPS: means Intrusion Prevention System which is a system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Platform: means a foundation or environment that enables software applications, services, or systems to run, develop, and interact.

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.

Key Vault: means a cloud-based service that helps securely store and manage secrets, encryption keys, and certificates.

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.

PAM: means Privileged Access Management which is the combination of tools and technology used to secure, control and monitor access to an organization's critical information and resources.

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.

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.

RPO: means Recovery Point Objective which is the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed as an amount of time.

SAML: means Security Assertion Markup Language which is an open standard that enables to access multiple web applications using one set of login credentials. It can be used to provide Single Sign-On (SSO) capabilities.

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

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

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

open-source components licenses in a codebase. This analysis is performed to evaluate security, license compliance, and code quality.

Service: means SITA WorldTracer® Bag Mate service.

AVD: means Azure Virtual Desktop which is a Microsoft Azure-based system for virtualizing its Windows operating systems, providing virtualized desktops and applications securely in the cloud.

API: means Application Programming Interface which is a set of protocols and tools that allow different software applications to communicate with each other.

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.

Hardening: means a process of securing a system, application, or network by reducing its vulnerability surface. This is done by eliminating unnecessary services, configurations, and access points, and by applying security best practices to protect against threats.

SSO: means Single Sign-On is an authentication mechanism that allows users to access multiple applications and websites using a single set of login credentials, such as a username and password.

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.

SSH: means Secure Shell Protocol which is a cryptographic network protocol for operating network services securely over an unsecured network.

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

Hardening: means a process of securing a system, application, or network by reducing its vulnerability surface. This is done by eliminating unnecessary services, configurations, and access points, and by applying security best practices to protect against threats.

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.

OS: means An Operating System which is system software that manages computer hardware, software resources, and provides common services for computer programs.

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.

Docker: means an open-source containerization platform that allows developers to package applications and their dependencies into a standardized unit called a container.

DevOps: means software development methodology that combines software development (Dev) and IT operations (Ops) to improve and shorten the systems development life cycle.

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.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

3. Security Technical and Operational 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 these TOMs.

3.2. SITA WorldTracer® Bag Mate specific security measures

The below security measures are implemented at SITA WorldTracer® Bag Mate 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.
  - The production environment is segregated from non-production environment, development and QA environments are also segregated
  - Logical segregation is achieved using tenantID, ensuring clear boundaries between tenants.
- Firewalls:
  - Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) firewall for traffic between platform ingress & egress points and the remote hosts
  - Web Application Firewalls for traffic between the customer applications and platform ingress point
- Network authentication: using protocols such as: Oauth2, Azure Active Directory

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:

- Antivirus: Containers are scanned as part of the CI/CD pipeline process.
- Vulnerability management: vulnerability management process is in place to remediate vulnerabilities. Vulnerability scans are performed monthly. Penetration tests are carried out on an annual basis.
- The security team receive 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.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

- Patch management: Patch management is part of the change management process to support hardening against security threats. In the case of updates to correct known vulnerabilities, critical security patches are prioritized and applied after identification.

  Patches are made available by the vendors and are systematically tested before implementation in production
- Capacity management:
  - Capacity of the Cloud is gathered and analyzed to ensure product/service applications meet current and future consumption demands. Forecasted usage that exceeds capacity tolerances or identifies the need for system cleanup to optimize resources triggers the SITA Change Management Process.
  - Platform use trend is checked each quarter and monitoring tools are used to receive and fix any capacity alarm or issue that may affect the performance of the Platform
- System operating procedures
- Logging and monitoring: product logs collection and protection, log analysis through a SIEM for system security monitoring
  - Application, infrastructure as well as request logs are retained for3 months and are automatically deleted after 7 days
- System hardening: system hardening policy, process and procedure, hardening at asset installation, regular application of hardening baseline
  - Containers OS deployed on cloud are hardened according to CIS guidelines
  - Configuration management is performed by Platform Operations 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:

- Atlas MongoDB is secured using Transparent Data Encryption (TDE) with the AES-256-CBC algorithm.
- Data in transit encryption / secure information exchange: Personal data communication is encrypted using HTTPS (TLS 1.2 or above)
- Information deletion:
  - Information deletion is governed by the SITA Global Data Retention Policy:
    - The retention time is set to 3 months
    - SITA shall delete all data without further notice to the customer within 1 day following the end of the configured data retention period; an automatic dedicated job is launched as soon as the data retention period has passed.
- 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.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

- 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.
  - Multi-factor authentication (MFA) is implemented for administration connection using Azure Virtual Desktops (AVD) and Palo Alto Prisma
- API Access management:
  - Best practice authentication (Oauth2 - client credentials flow (server))
  - User lists and permissions are reviewed on a yearly basis for applications/services.
- Protection of authentication information: all passwords are stored encrypted,
  - Secure software is used to manage credentials, keys and passwords. Additional level of authentication is needed to access Azure Key Vault.
- Restricted access to source code: RBAC (Role Based Access Control) policy is implemented.
- PAM (Privileged Access Management): An administrative tool in Zendesk is used to grant any administrative privilege.
- Segregation of duties (SoD): A segregation of duties is implemented. The operation team is separated from the development team, and an administrator role is defined for privileged access.

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.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

  - 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,
- API security: OAuth 2.0 token-based authentication is implemented.

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:

- Data backup: Cloud-based backup with Atlas MongoDB database.
- Data backup protection: Data backups are encrypted using keys stored in Azure Key Vault.
- A disaster recovery plan exists. The service can be restored in 4 hours in a disaster recovery datacentre if the active datacentre is down. The Recovery Point Objective or the maximum amount of data that can be lost after a recovery from a disaster corresponds to 1 hour.
- Systems redundancy: Multiple Docker container instances are utilized to implement our microservices architecture, enabling modular deployment and efficient scalability
- 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 Datacenter security

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

- Datacenter access restrictions: standard Microsoft Azure security measures are implemented, please refer to Microsoft Product and Services DPA protection addendum – Appendix A – Security Measures
- Data availability: Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are documented and agreed upon within agreements with Customers.
- Cloud infrastructure redundancy: Microsoft Azure cloud is deployed across multiple availability zones within the same region.
- The Service is running on Azure Cloud and rely on Microsoft security.

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential

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)

© 2025 SITA Switzerland Sarl – All rights reserved – Confidential