Security Technical and Organizational Measures (TOM) Appendix for SITA WorldTracer Auto Reflight 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 inconsistency 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 which is a set of programming code 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.

CDN: means Content Delivery Network which is a geographically distributed group of servers that work together to provide fast delivery of Internet content.

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.

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.

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.

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.

JWT: means JSON Web Token which is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

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.

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.

PII: means Personally Identifiable Information which is 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 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.

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 WorldTracer Auto Reflight

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.

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

TOMs: means Technical and Organizational Measures 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 WorldTracer Auto Reflight specific security measures

The below security measures are implemented at SITA WorldTracer Auto Reflight service level:

3.2.1. Network security

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

- Network segmentation: security groups, resources groups and availability zones are used and configured to ensure network segmentation is appropriately enforced,
- Content Delivery Network: Amazon CloudFront is enabled,
- Network devices hardening: all environments are built based on a CIS Benchmark hardened image,
- Firewall, VPN: SITA WorldTracer Auto Reflight being hosted in AWS, please refer to AWS GDPR Data Processing Addendum – Annex 1 – AWS Security Standards, available on AWS Whitepaper webpage.

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: a vulnerability management procedure is documented and implemented:
  - Vulnerability scans are performed every 3 weeks using standard SITA tools and vulnerability assessments and penetration tests are launched once every year,
- Patch management: a patch management procedure is documented and implemented:
  - A specific pipeline is used for patching: patches are systematically tested before being implemented into production,
- Change management: a change management procedure is documented and implemented:
  - An ITSM tool is used to track all changes; all changes go through the Change Approval Board (CAB) process,
- Capacity management: Amazon CloudWatch is used for operational monitoring; performance is assessed through dedicated metrics and dashboards; systems can be sized horizontally and vertically,
- System operating procedures: standard system operating procedures are documented,
- Logging and monitoring: application logs are collected and analyzed in Amazon CloudWatch with alarms triggered in case on suspicious or forbidden event; NTP is in place for clock synchronization; manual logs analysis is also performed in case of troubleshooting; log retention is set to 21 days; once the retention period has passed, the logs are automatically deleted using a daily job,

- SITA WorldTracer Auto Reflight being hosted in AWS, for additional information on capacity management and system hardening, please refer to AWS GDPR Data Processing Addendum – Annex 1 – AWS Security Standards, available on AWS Whitepaper webpage.

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:

- Data classification: all the data in the application is classified as PII hence the same level of security is applied to all the hosted data,
- Data at rest encryption: disk encryption is implemented,
- Secured information exchange / data in transition encryption: HTTPS (TLS 1.3) is implemented for all data in transit (both internal traffic and ingress/egress traffic). TLS1.0 and 1.1 have been disabled; APIs are secured with a dedicated API gateway with TLS 1.2,
- Information deletion: a data retention policy is documented and implemented:
  - The retention period is set to 60 days,
  - SITA shall delete all data without further notice to Customer within 10 days following the end of the 60-day data retention period,
  - An automatic and daily purge using dedicated jobs is launched as soon as the data retention period has passed.

References	
Related ISO/IEC 27002:2022 controls	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:

- Access management: access management and review procedures are documented, reviewed and updated regularly:
  - When a user wants to access an application or an AWS account, a defined process must be followed for access request,
  - Access recertification is performed twice a year,
- Authentication: password policy and complexity rules are documented and implemented:
  - Unique usernames are used for all AWS users and administrators; any account inactive for 30 days is deactivated and an administrator action is required to reactivate it; an anti-brute force attack mechanism is implemented and relies on MFA; password expiration time set to 30 days by default; log out time is set to 30 minutes by default (configurable by the Customer),
- Multi-factor authentication (MFA): the root user and all users must use MFA to access AWS console, if they have it enabled,
- Protection of authentication information: passwords are set up by SITA support team and sent by e-mail using encrypted e-mail solution; passwords are encrypted; in case of forgotten password, a call to an administrator is required to verify the identity prior to trigger the password reset,

- Restricted access to source code: access to source code is restricted based on RBAC model and least privilege,
- Privileged Access Management (PAM): a PAM policy is implemented:
    - AWS Console accounts are the only privileged users identified and are secured based on RBAC model, with dedicated accounts and MFA for authentication; a bastion is implemented,
- Segregation of Duties (SoD): user groups and specific user roles have been defined and ensure SoD enforcement.

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: 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/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25),
- Vulnerability scanning: vulnerability scans and assessments are launched before each code release using a dedicated tool,
- Penetration testing: penetration tests are performed on a yearly basis by security team,
- API security: APIs are secured through API secure gateway (TLS 1.2) and JWT token-based authentication.

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: a backup policy and a backup process are implemented:
    - Full daily databases backups are performed,
    - Data backup retention period is set to 30 days,
    - SITA shall delete all data backup without further notice to Customer within 10 days following the end of the 30-day 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,
    - A monitoring process is in place to ensure the purging process is properly triggered,
- Data backup protection: data backups are stored on a storage separated from production environment,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

- Systems redundancy, disaster recovery plan, disaster recovery testing: SITA WorldTracer Auto Reflight being hosted in AWS, please refer to AWS GDPR Data Processing Addendum – Annex 1 – AWS Security Standards, available on AWS Whitepaper webpage.

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:

- Datacenter access restriction: SITA WorldTracer Auto Reflight being hosted in AWS, please refer to AWS GDPR Data Processing Addendum – Annex 1 – AWS Security Standards, available on AWS Whitepaper webpage.
- Cloud redundancy: it is implemented using different availability zones in AWS, allowing seamless failover.
- Cloud backup recovery: Recovery Time Objective (RTO) is set to 120 minutes and achieved using availability zones with replication between the databases; No RTO is set as no data loss shall occur for a localized outage.

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)