

Security Technical and Organizational Measures (TOM) Appendix for SITA WorldTracer Tablet 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:

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

AES means Advanced Encryption Standard which is a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

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.

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.

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.

CPU means Central Processing Unit which is the component of a computer system that controls the interpretation and execution of instructions.

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.

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 tool 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.

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

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.

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 which is the 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.

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 model 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 are 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 Tablet

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.

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.

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.

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.

VM means Virtual Machine which is a software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.

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 Tablet specific security measures

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

3.2.1. Network security

The below specific network security measures are implemented for SITA WorldTracer Tablet:

- Network segmentation: VLAN segmentation is implemented,
- Reverse proxy: a reverse proxy is implemented,
- Firewall: next-gen security firewalls are implemented for SSH traffic; ATI Cloud edge firewalls are also in place,
- VPN: remote access VPN and client VPN for SSH are implemented,
- Network devices hardening: SSH is enabled with TLS 1.2; hardening measures are implemented using hardened image based on CIS benchmark; other unnecessary services running on Linux machines are disabled; robust password policies are enforced,
- Network authentication: network authentication relies on protocols such as Kerberos and LDAP/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 SITA WorldTracer Tablet:

- Antivirus: antivirus is deployed on all VMs and servers,
- 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 quarter,
- Patch management: a patch management procedure is documented and implemented:
 - ▶ Patches are gathered from different sources and are systematically tested before implementation in production; industrialized patching is implemented,
- 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: a capacity management process is documented and implemented:
 - ▶ Monitoring tools (scripts) are used to assess and alert on any capacity issues on network equipment and servers (CPU, memory utilization, resource utilization),

- System operating procedures: standard system operating procedures are documented,
- Logging and monitoring: server logs and applications logs are collected and reviewed using monitoring tools and manual analysis; NTP is in place for clock synchronization; logs are stored on servers with size-based rotation; a log retention policy is implemented with 7 days retention period for standard logs and 30 days retention for security logs; audit logs are retained for 6 months; no PII data is stored within those logs,
- System hardening: hardening activities are performed using SITA catalogue hardened images (based on CIS benchmark).

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 SITA WorldTracer Tablet:

- Data classification: data is classified according to SITA Data Classification Policy and documented in ad hoc security documentation,
- Secured information exchange / data in transition encryption: HTTPS (TLS 1.2) is implemented for all information exchanges,
- Data at rest encryption: application-level encryption is implemented and based on AES-256 mechanism,
- Data desensitization: data used in development is simulated or provided anonymized for specific scenarios,
- Information deletion: WorldTracer Tablet does not store transactional data permanently, a regular push and purge to SITA WorldTracer Open is performed.

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 SITA WorldTracer Tablet:

- Authentication: password policy and complexity rules are documented and implemented:
 - The application has a configuration for number of failed login attempts after which the account would be locked; the password expiration time is set to 30 days; a configurable inactive session logout (30 minutes by default) is also implemented,
- Conditional access: location restriction is implemented for client VPN access,
- Protection of authentication information: passwords are set up by SITA support team and sent by e-mail using the encrypted corporate e-mail server; passwords must be changed at first login,
- Restricted access to source code: access to source code is restricted using the implemented RBAC model,
- Privileged Access Management (PAM): a PAM policy is implemented:
 - A bastion solution and a VPN are implemented,
- Segregation of Duties (SoD): access requests to production environment must be approved by SITA IMS Operations team; system accounts SoD is reviewed every quarter.

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 SITA WorldTracer Tablet:

- Secure coding: a secure coding policy is documented and implemented:
 - ▶ It is shared by CISO and followed by developers; a secure coding checklist is used including scans and contractual requirements with third parties; some peer code reviews are performed within the development teams; 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 quarterly basis by security team,
- Secure CI/CD platform: a privately hosted platform is used, with VPN required to connect to it,
- API security: APIs are secured through the API secure gateway (TLS 1.2) and using 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 SITA WorldTracer Tablet:

- Data backup: a backup policy and a backup process are implemented (relying on SITA WorldTracer Open, as SITA WorldTracer Tablet does not store transactional data permanently, a regular push (purge) to WorldTracer Open being performed):
 - ▶ Full database backups are performed daily; VMs are also backed up,
 - ▶ Data backup retention period is set to 7 days,
 - ▶ SITA shall delete all 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 backup data 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: backups are segregated from the production environment,
- Systems redundancy: infrastructure redundancy is in place through clustered services (Active-Active) to ensure high availability,
- Disaster recovery plan: a backup and restore plan is implemented:
 - ▶ Staging environment is used for disaster recovery,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

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 SITA WorldTracer Tablet:

- Datacenter access restriction: a cloud security policy is in place with strict restrictions implemented:
 - Access control lists that define what resources users are permitted to access; closed circuit video equipment coverage at the facility perimeter at all access control points; security camera monitoring; facility-based security video data recorded and retained for at least 90 days; datacenter access restricted with MFA; 24x7x365 onsite security staff providing additional protection against unauthorized entry; audit trails, log collection and monitoring; regular physical security independent audits.
- Cloud infrastructure redundancy: SITA ATI Cloud infrastructure is a highly redundant infrastructure including compute, network redundancy, storage and management plane redundancies, and ensuring resiliency and high availability.
- Cloud backup recovery testing: a dedicated solution is used to perform data backups of critical datacenter management systems and to monitor the backups for completion status; backups are stored offsite via cloud infrastructure managed through the dedicated solution; on a daily basis, a report evidencing the success or failure of each scheduled backup is generated; Recovery Time Objective (RTO) is set to 120 minutes; Recovery Point Objective (RPO) is not set as SITA WorldTracer Tablet does not store any transactional data.

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)