

Security Technical and Organizational Measures (TOM) Appendix for SITA Airport Management System (AMS) Anywhere service schedule

Version: September 2024

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 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:

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 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.

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

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.

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.

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.

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.

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 AMS Anywhere service.

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.

TDE: means Transparent Data Encryption which is an encryption of database at file level to secure data at rest.

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 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 AMS Anywhere specific security measures

The below security measures are implemented at SITA AMS Anywhere.

3.2.1. Network security

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

- Network segmentation: micro-segmentation is implemented through Azure network security groups,
- Web application firewall: Azure Web Application Firewall (WAF) is implemented,
- Network devices hardening: TLS 1.2 and above is implemented, and robust password policies are enforced; Azure hardening standards are in place,

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 process is documented and implemented:
 - Penetration tests are performed at least once year,
- Patch management: a patch management process is documented and implemented:
 - Patch management activities are managed using Azure Update Manager (Update Management) tool,
- 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,
- Capacity management: a capacity management process is documented and implemented:
 - Monitoring and supervision tools are used to assess and alert on any capacity issues on network devices and servers (CPU, memory utilization, resource utilization),
- System operating procedures: standard operating procedures are documented,
- Logging and monitoring: Azure Monitor is used for logging and monitoring purposes; logs are stored in a dedicated Azure Storage; logs retention period is set to 30 days, with automated deletion as soon as the 30 days retention period is reached.
- System hardening: system is hardened using images provided by Microsoft based on CIS benchmark Level 1.

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:

- Secured information exchange / data in transit encryption: both ingress and egress traffic are performed through APIs over HTTPS using TLS 1.2 and above encryption,
- Data at rest encryption: by default, Azure Disk Encryption and Transparent Data Encryption (TDE), are implemented
- Information deletion: AMS Anywhere does not store any data except configuration logs, and no personal data is stored

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:
 - For Customers users, Azure AD B2C authentication is used, however, the password policy, the password complexity rules and the account expiration configuration remain under the Customer's responsibility.
 - For SITA support users, Azure AD authentication is also used, with SITA password policy enforced, including a 3-month expiry time; account lockout capabilities are also enabled.
- If customer Multi-factor authentication (MFA) is integrated:
 - Multi-factor authentication (MFA): a token-based MFA using OAuth 2.0 protocol is implemented and used by SITA support users. It is Customers' responsibility to enable MFA for their users
- If customer Single Sign-On (SSO) is integrated:
 - Single Sign-On: OpenID Connect (OIDC) protocol against client's identity provider (IdP) is used for SSO purpose. SSO is enabled for SITA support team.
- Restricted access to source code: access to source code is restricted based on RBAC model and least privilege,
- Privileged Access Management: a privileged access management policy is implemented for SITA support team. A bastion is in place and a RBAC model is used. There are no privileged accounts on Customers' side, as only 1 type of account exists (employee),
- Segregation of duties (SoD): SoD is implemented using RBAC model in Azure Pipelines, with different roles to push and approve code.

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:

- Web application firewall: Azure Web Application Firewall (WAF) is enabled on Azure Application Gateway,
- Secure coding: a secure coding policy is documented and implemented:
 - A secure coding checklist is used.
 - 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.
 - External development team (if involved) forms an integral part of the SITA development team and follows similar secure coding practices.
- Penetration testing: penetration tests are performed at least once a year,
- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions on who can run the pipeline and promote the code,
- API Security: Azure Application Gateway 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:

- Systems redundancy: Active/Active failovers is in place,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.
- Data backup: Azure SQL DB backup process is implemented.
- Data backup protection: backups are encrypted in Azure SQL using Transparent Data Encryption (TDE).

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.
- Azure Advisor security baseline is used, and recommendations followed and implemented.

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)