

Security Technical and Organizational Measures (TOM) Appendix for SITA API PNR Gateway Portal

Version: November 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:

CIS: CIS benchmarks hardening guidelines, 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: Continuous Integration (CI) and Continuous Development (CD): CI 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.

SAST, DAST and/or SCA: means 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 API PNR Gateway Services.

VPN: a 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 API PNR Gateway Portal specific security measures

The below security measures are implemented for the SITA API PNR Gateway Portal:

3.2.1. Network security

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

- Network segmentation:
 - o Firewall segmentation to separate different service tiers such as development, pre-production and production.
 - o Segmentation of application functionality to minimise connectivity between messaging activities, data activities and application processing activities.
 - o External traffic is terminated outside of the main application service and in a segregated network partition.
 - o External messaging traffic is delivered over private service networks.
- Network Encryption
 - o Data exchanged with customer sites is encrypted based on customer requirements.
- VPN is used to restrict, secure, audit and manage remote access:
 - o remote access to the service for operations and support staff is via VPN
 - o Where required by a customer a site-to-site VPN may be used to encrypt and authenticate access.
- Network devices are hardened (disabling of unnecessary services and protocols, enforcement secure access to the console, enforcement of robust password policies, control of access lists for remote administration, restrictions of physical access to routers and switches, back up configurations, test security configurations).
- Network interactions are authenticated using a combination of mutual certificates, and user credentials.

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 is deployed for all servers that are used in the service.
- Vulnerability management: a vulnerability management process is documented and implemented:
 - o Environment vulnerability scans are performed; penetration tests are performed at least once a year,
 - o Software is scanned during the CI/CD process whenever software changes are released.

- Patch management: a patch management process is documented and implemented:
 - o A team is in place and relies on industrialized patching tools; all security patches are tested and certified in a test environment before being deployed in production,
- Change management: a change management procedure is documented and implemented:
 - o 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:
 - o Monitoring and supervision tools are used to assess and alert on any capacity issues on network devices and servers (CPU, memory utilization, resource utilization).
 - o Traffic loads are recorded and monitored for the purpose of capacity planning.
 - o As new customers are on-boarded an assessment of the additional traffic is performed.
 - o Load testing identifies the capacity of the service.
- System operating procedures: standard operating procedures are documented,
- Logging and monitoring: Server access is logged and audited.
- All hosts are hardened to CIS Level 1.

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; 08.09. Configuration management; 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
 - o Data is classified based on its sensitivity and owner of the data
- Data at rest encryption is applied for all databases.
- Disk level encryption is enabled for all application services.
- TLS encryption is applied to all network traffic received over public networks.
- All messaging data into and out of the service is via trusted networks, either via SITAs MPLS Service networks, or encrypted tunnels. TLS encryption is applied where possible.
- Traveller personal data is deleted once it is no longer required for the processing of traveller assessments, and this personal data shall not be stored for a period longer than 7 days. After this time, the traveller personal data shall be deleted by SITA without further notice to the customer.

References	
Related ISO/IEC 27002:2022 controls	05.12. Classification of information; 05.13. Labelling of information; 05.14. Information transfer; 08.10. Information deletion; 08.11. Data masking; 08.12. Data leakage prevention; 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:

- Customer access to the service is controlled via username/password authentication and must adhere to predefined security policies.
- Customers are responsible for their user management policies and procedures.
- Operations and support access is authenticated (and supporting password policy, enforcement of password complexity rules, account sessions management with account locker, log out time)
- Conditional access is controlled through VPN/Microsoft Active Directory.
- Protection of authentication information: initial account creation is managed by SITA, with mandatory change of password by the user at first login,
- Restricted access to source code (role-based access, fine-grained permissions management, regular permissions review, access linked to SITA corporate user access)
- Segregation of duties (SoD) is implemented using group policies

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 (secure coding policy, process and procedure, secure software development lifecycle management, automated SAST, DAST and/or SCA code review tools, standardized peer review)
- Security architecture review by application and infrastructure security architects.
- Vulnerability scanning at software release (regular exposed assets vulnerability scanning)
- Penetration testing (regular exposed assets penetration testing)
- Threat modeling using Microsoft Threat Modeling Tool: Reviewing threats and ensuring appropriate mitigations are 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 (data incremental backups, offsite backups)
- Data backup protection (backups segregated from production environment, backup encryption)

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 Measures

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

- Datacenter access restriction: a cloud security policy is in place with strict restrictions implemented:
 - o 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; data centre access restricted with Multifactor Authentication (MFA); 24x7x365 onsite security staff providing additional protection against unauthorized entry; audit trails, log collection and monitoring; regular physical security independent audits.

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);