Security Technical and Organizational Measures (TOM) Appendix for SITA Flex Hybrid service schedule

Version: October 2023

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 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:

CAB: means Change Advisory Board which is the managerial instance supporting the assessment, prioritization, authorization, and scheduling of changes.

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.

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.

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.

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.

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.

Radius: means Remote Authentication Dial-In User Service which is an authentication, authorization, and accounting protocol that manages network access.

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 Flex Hybrid service.

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.

TACACS+: means Terminal Access Controller Access-Control System Plus which is a security protocol handling remote authentication and related services for network access control through a centralized server.

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

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.

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 Flex Hybrid specific security measures

The below security measures are implemented at SITA Flex Hybrid.

3.2.1. Network security

The below specific network security measures are implemented for the Service independent of deployment option:

- Network segmentation: VLAN segmentation, firewall segmentation
- Outbound connectivity to the Internet for accessing Cloud resources via Azure Front Door is secured at the airport by next gen firewall policies and distributed proxy whitelisting for content filtering.
- Inbound connectivity initiated from either the private WAN or Internet services to Flex locations is not permitted.
- VPN: site-to-site VPN for connection between hub & satellite sites where applicable; remote access VPN for remote support teams and for connectivity of devices over wireless networks where applicable
- Network devices hardening: enabling of SSHv3 or TLS, disabling of unnecessary services and protocols, enforcement secure access to the console, enforcement of robust password policies, control of access lists for remote administration, restrict physical access to routers and switches, back up configurations, test security configurations
- Network authentication: using protocols such as: TACACS+, RADIUS, Kerberos, LDAP/Active Directory
- If SITA Flex Hybrid is deployed using **"Core Room" hosted** option:
    - Domain services and airport inventory management are hosted on-prem in the Airport core room, access is controlled via Firewall policies. Only outbound connectivity is permitted for replication and remote supervision.
- If SITA Flex Hybrid is deployed using **"Serverless" hosted** option:
    - Outbound connectivity to Cloud resources for domain services and airport inventory management is secured via local common services (Next Gen) firewalls.

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: for clients and for servers.

- Vulnerability management: vulnerability management process and procedure, vulnerability scanning (Tenable), penetration testing
- Vulnerability scans are in place for new images at every new release
- Patch management: patch management policy, process and procedure
    - Patch management activities managed using Azure Patch Manager (Update Management) tool. The patches are assessed by Integration team for applicability.
- Change management: change management policy, process and procedure, use of an ITSM tool, Change Advisory board (CAB)
    - Azure DevOps tool is used to track and perform all the software changes with a defined approval process.
    - SITA Operations use an ITSM tool to manage the operational changes. High Risk Changes require a GO from the CAB.
- Capacity management: capacity management policy, process and procedure
    - Monitoring/supervision tools are in place to detect or anticipate any capacity issue on network devices and servers (number of requests, bandwidth use, CPU, memory utilization, resource utilization)
- System operating procedures: standard operating procedures are documented,
- Logging and monitoring: product logs collection and protection
    - If SITA Flex Hybrid is deployed using **"Serverless" hosted** option: Azure Log analytics is in place to manage logs in Azure (retention period set by default to 90 days).
    - SIEM collects logs and correlates them for further analysis; data can be kept up to 1-year retention (customizable).
- System hardening: system hardening policy, process and procedure, hardening at asset installation, regular application of hardening baseline (e.g., deleting unneeded drivers, restricting peripherals, encrypting host drive, restricting system access privileges) on servers, OS, middleware and database, automatic assets scans to assess hardening requirements
- Hardening policy exists for the servers in the cloud. The images are hardened following Center for Internet Security (CIS) Level 1 security hardening for Windows Operating Systems.

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:

- Application logging at Flex locations (workstations and kiosks) includes PNR data as required for troubleshooting purposes only. This data is purged every 48 hours by an automated script.
- Data at rest encryption: application-level encryption, database encryption, file system encryption, full disk encryption
- Secured information exchange / Data in transit encryption: secured and accepted protocols (TLS 1.2), industry standard encryption mechanism (AES-256)

- Information deletion: data retention period (up to 90 days for billing data without PII; and 48 hrs for logs files with PII), process and procedure, automatic data purging with scripts.

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 authentication for APIs, SITA Privileged Users with password policy, enforcement of password complexity rules, account sessions management with account locker, log out time
    - Conditional access controls are implemented using group policies in Active Directory
    - Privileged Access Management: Unique account per SITA Privileged User
- SoD for SITA Privileged Users accessing the system remotely: SoD policy, process and procedure, SoD matrix, account creation and access rights validation process ensuring SoD
- SoD is implemented to allow end customers to access only the applications they are authorized to use
- Note: Airline & Ground Handler user accounts are generic following an IATA defined standard based on the customer and location IATA codes and used for presentation purposes, not access control and authentication

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 SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25);
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle.
- Penetration testing: penetration tests are performed at the application level before each release; additional tests are performed in case of major updates,
- Secure CI/CD platform: Azure DevOps Pipelines and Terraform are used, with restricted permissions on who can run the pipeline and promote the code,
  API security: APIs are secured using bearer token-based access.

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 backup policy, process and procedure, backup scheduling, on-premises backup, cloud-based backup.
    - If SITA Flex Hybrid is deployed using **"Core Room" hosted** option: a weekly full backup with daily incremental backup policy to meet the contracted SLA.
    - If SITA Flex Hybrid is deployed using **"Serverless" hosted** option: SITA is currently using an Azure Backup policy that performs daily full backups on all the IaaS VM's with seven days retention period, but this may be adjusted to meet the contracted SLA.
- Crisis management: crisis management policy, process and procedure, crisis management tooling (e.g., ad hoc communication paths, reflex cards, emergency button)
- The SITA Flex cloud infrastructure is a set of regional cloud instances that are geographically spaced around the globe. Each SITA Flex instance ("Core") is deployed in selected Azure regions according to the requirements of connected SITA Flex Hybrid sites. Each Flex Core has a designated backup/fail-over Core for DR. Each Azure Flex Hybrid Region support multiple airports within latency guidelines where capacity is monitored and adjusted over time.

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.
- Cloud redundancy capabilities: hardware redundancy and geographic redundancy as per agreed SLA.

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)