Security Technical and Organizational Measures (TOM) Appendix for Smart Path service schedule

Version: April 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.

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.

IDS: means Intrusion Detection System which is a device or software application that monitors a network or systems for malicious activity or policy violations.

IPS: means Intrusion Prevention System which is a system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

IP: means Internet Protocol which is the principal communications protocol in the IETF Internet protocol suite for specifying system address information when relaying datagrams across network boundaries.

IPVPN: means Internet Protocol-based Virtual Private Network which is a seamless connectivity across multiprotocol label switching between a private network and remote users.

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.

MPLS: means Multiprotocol Label Switching which is a networking technology that routes traffic using the shortest path based on labels rather than network addresses, to handle forwarding over private wide area networks.

SSL: means Secure Socket Layer which is a security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

NTP: means Network Time Protocol which is an internet protocol used to synchronize with computer clock time sources in a network.

OVA: means Open Virtual Machine format which is an open standard for packaging and distributing virtual appliances or, more generally, software to be run in virtual machines.

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.

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

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.

RPO: means Recovery Point Objective which is the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed as an amount of time.

SAML: means Security Assertion Markup Language which is an open standard that enables to access multiple web applications using one set of login credentials. It can be used to provide Single Sign-On (SSO) capabilities.

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 Smart Path service.

SFTP: means SSH File Transfer Protocol which is a secure file transfer protocol that uses secure shell encryption to provide a high level of security for sending and receiving file transfers.

SHA: means Secure Hash Algorithm which is a hash algorithm with the property that it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest.

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 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. Smart Path specific security measures

The below security measures are implemented at Smart Path level. Smart Path consists of Smart Path Client and Smart Path Hub (SPH).

3.2.1. Network security

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

Smart Path Hub (SPH) - On-premises (SITA managed) hosted:

- Network segmentation: VLAN segmentation, Firewall segmentation
- Firewall: server-based firewalls are implemented and managed by SITA network team,
- Secure Web Gateway (SITA Community Connect Internet) to restrict Internet traffic (access control lists, web filtering)

Smart Path Client:

- Smart Path Client uses the services of Smart Path Hub systems.
- Network segmentation: VLAN segmentation, Firewall segmentation is implemented at airport.

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:

Smart Path Hub (SPH) - On-premises (SITA managed) hosted:

- Antivirus: antivirus is deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
    - Environment vulnerability scans are performed,
- Patch management: a patch management process is documented and implemented:
    - A dedicated team is in place and relies on industrialized patching tools; 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:
    - 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,
- System hardening: a system hardening policy and checklist is documented and implemented:
    - Servers are hardened based on CIS benchmark.
- Hardware security: server is deployed in Airports data centre; premises are secured by airport authority.
- Logging and monitoring: SPH logs collection and protection is implemented.
- NTP is in place for clock synchronization.

Smart Path Client:

- Antivirus: antivirus is deployed on workstation,
- Patch management: a patch management process is documented and implemented:
    - A dedicated team is in place and relies on industrialized patching tools; 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:
    - An ITSM tool is used to track all changes; all non-standard changes go through the CAB process,
- System operating procedures: standard operating procedures are documented,
- System hardening: a system hardening policy and checklist is documented and implemented:
    - Workstations are hardened based on CIS benchmark.
- Hardware security: kiosks deployed in Airports premises are secured by a locked box.

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:

Smart Path Hub (SPH) - On-premises (SITA managed) hosted:

- Data at rest encryption (MS SQL database TDE encryption)
- Data in transit encryption / secure information exchange: personal data communication is encrypted using HTTPS (TLS 1.2 or above)
- Information deletion: a data retention policy is documented and implemented:
    - No personal data (PII) is stored permanently in the product,
    - The retention time is set to 3 days by default; retention period is configurable for customer based on agreed requirements,
    - SITA shall delete all data without further notice to the customer within 1 day following the end of the configured data retention period; an automatic dedicated job is launched as soon as the data retention period has passed.

- Data desensitization: Logs are anonymized.

Smart Path Client:

- No personal data (PII) is stored permanently in the client.
- Troubleshooting logs are kept for 72hrs; configurable for customer based on agreed requirements.

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:

Smart Path Hub (SPH) - On-premises (SITA managed) hosted:

- Authentication:
  - Active Directory is used for authentication using OAuth 2.0.
  - A strong authentication policy is implemented; token expiry time is configured.
- Protection of authentication information: all passwords are stored encrypted,
- Multi-factor authentication: MFA is implemented to ensure restricted access to source code and in addition to the VPN, for remote administration and support to on-premises environment by SITA administrators,
- Log-out time is also implemented for remote access to the server,
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC model and based on MFA implementation,
- Segregation of duties (SoD): SoD is implemented using RBAC model: several roles and account types are used to respect the principle of least privilege,

Smart Path Client:

- Uses SPH provided authentication.
- Multi-factor authentication: MFA is implemented to ensure restricted access to source code and in addition to the VPN, for remote administration and support to on-premises environment by SITA administrators,
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC model and based on MFA implementation,

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:

Smart Path Hub (SPH):

- Secure coding: a secure coding policy is documented and implemented:
    - It is shared by SITA information security team and followed by developers; a secure coding checklist is used including scans,
    - A DevOps guide is provided to the developers and describes a list of best practices regarding secure coding, data protection and security development measures.
    - 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.
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle, before each code release,
- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions on who can run the pipeline and promote the code; deployment requires an approval process,
- API security: OAuth 2.0 token-based authentication is implemented.

Smart Path Client:

- Uses SPH provided authentication.
- Secure coding: a secure coding policy is documented and implemented:
    - It is shared by SITA information security team and followed by developers; a secure coding checklist is used including scans,
    - A DevOps guide is provided to the developers and describes a list of best practices regarding secure coding, data protection and security development measures.
    - 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.
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle, before each code release,
- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions on who can run the pipeline and promote the code; deployment requires an approval process.

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:

Smart Path Hub (SPH) - On-premises (SITA managed) hosted:

- Data backup: a data backup policy is documented and implemented:
    - Database are backed up through daily full backups and hourly transactional backups,
    - The data backup retention time is **14 days** by default for daily full backups (can go up to 30 days on request) and **2 days** for transactional backups; servers are backed up daily with 14 days retention period,
    - SITA shall delete all data backup without further notice to Customer within **10 days** following the end of the configured backup data retention period,

    - File data is controlled through an automated SQL backup job allowing deletion as soon as the retention is reached; database data is controlled through automated application configuration allowing deletion as soon as the retention is reached,
- Data backup protection: backups are segregated from the production environment; backups are encrypted,
- Systems redundancy: application redundancy is in place through clustered services (Active-Active) to ensure high availability,
- 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	08.14. Redundancy of information processing facilities
Related GDPR principles	Storage limitation; Integrity and confidentiality (security)