Security Technical and Organizational Measures (TOM) Appendix for Airport Vision (APV) Service Schedule

Version: September 2025

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 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.

CIS benchmarks hardening guidelines: means 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.

Least Privilege: means a security concept that involves granting users the minimum level of access or permissions necessary to perform their job functions.

Need To Know: means a security principle that ensure individuals have access to only the information and resources they require to perform their duties effectively

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.

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

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.

SLA: means for Service Level Agreement is a contract that defines the services to be provided, expected performance levels, and how performance will be measured.

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.

UAT: means User Acceptance Testing is a phase in the software development process where the end users or clients test the software to ensure it meets their requirements and works as expected.

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 APV service.

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.

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.

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. APV specific security measures

The below security measures are implemented at APV level. APV consists of APV Web Client and APV Display Client.

3.2.1. Network security

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

APV is deployed using **SITA managed on-premises hosted**:

- Network segmentation: VLAN and firewall segmentation is implemented to isolate APV from rest of the network
- Firewall: software-based and network-based firewalls are implemented
- Network devices hardening: SSH is enabled with TLS 1.2; hardening measures are implemented

APV is deployed using **Customer managed hosted**:

- Network segmentation: VLAN and firewall segmentation is advised to isolate APV from rest of the network
- Firewall: software-based and network-based firewalls are advised
- Network devices hardening: SSH is enabled with TLS 1.2; hardening measures are implemented
- Web application firewall: a network based WAF can be implemented at customer level on customer's request.
- APV Display Client:
- Server based Firewall segmentation is implemented at airports.

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:

APV is deployed using **SITA managed on-premises hosted**:

- Antivirus: antivirus is deployed on servers

- Patch management: Manual patching is enforced; all patches are tested before moving to UAT or production

- Change management: a change management procedure is documented and implemented:
  - An ITSM tool is used to track all changes; all changes go through the CAB process,

System operating procedures: standard operating procedures are documented for administration and support, including standard security configurations,

- System hardening: pre-hardened deployment are performed based on SITA recommendations

APV is deployed using **Customer managed hosted**:

- Antivirus: antivirus is deployed on servers
  - Patch management: Manual patching is enforced; all patches are tested before moving to UAT or production
- Change management: a change management procedure is documented and implemented:
  - An ITSM tool is used to track all changes; all changes go through the CAB process,
- System operating procedures: standard operating procedures are documented for administration and

support, including standard security configurations,

- System hardening: pre-hardened deployment is performed based on SITA recommendations

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:

APV is deployed using **SITA managed on-premises hosted**:

Data at rest encryption: no personal data are recorded; all passwords are encrypted.

Information deletion: default data retention policies are implemented

Data deletion is automatically performed through a dedicated SQL job as soon as the data retention period is reached. A job is launched on a daily basis and deletes all the reports that expired. The default is 30 days but it can be configured to be more or less.

APV is deployed using **Customer managed hosted**:

Data at rest encryption: no personal data are recorded; all passwords are encrypted.

Information deletion: default data retention policies are implemented.

Data deletion is automatically performed through a dedicated SQL job as soon as the data retention period is reached. A job is launched on a daily basis and deletes all the reports that expired. The default is 30 days but it can be configured to be more or less.

APV Display Client: APV Display client is a display only application and no data is recorded.

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:

APV is deployed using **SITA managed on-premises hosted**:

Authentication: In case of manual authentication, password policy and complexity rules are documented and implemented. LDAP authentication based on the airport's Acitve Directory can be used instead of manual username/password:

A session timeout is in place. Timeout length can be configured on a group level and per user level. It is also possible to specify a "never timeout" option.

Restricted access to source code: access to source code is restricted based on the RBAC model implemented.

Privileged Access Management: SITA applies a "Least Privilege" and "Need to Know" approach.

APV is deployed using **Customer managed hosted**:

Authentication: In case of manual authentication, password policy and complexity rules are documented and implemented. LDAP authentication based on the airport's Acitve Directory can be used instead of manual username/password:

A session timeout is in place. Timeout length can be configured on a group level and per user level. It is also possible to specify a "never timeout" option.

Restricted access to source code: access to source code is restricted based on the RBAC model implemented.

Privileged Access Management: SITA applies a "Least Privilege" and "Need to Know" approach.

APV Display Client:

As APV Display Client is a display only application no authentication is required.

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:

APV is deployed using **SITA managed on-premises hosted**:

- 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.

- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle, before each code release.

APV is deployed using **Customer managed hosted**:

- 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.
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle, before each code release.

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:

APV is deployed using **SITA managed on-premises hosted**:

Systems redundancy: application redundancy is in place through clustered services to ensure high availability as per agreed SLA.

Incident management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

Daily scheduled backups (full backups) are launched; backups are stored in a dedicated storage.

Data backup protection: backups are kept on a separate storage.

Retention period is typically 7 days, varying by site, but it can be customized based on customer requests.

APV is deployed using **Customer managed hosted**:

Systems redundancy: application redundancy is in place through clustered services to ensure high availability as per agreed SLA. It is possible to have an entire separate Disaster Recovery Environment (DRE) that is a copy of the production environment to be used in case of disaster.

Incident management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

Daily scheduled backups (full backups) are launched; backups are stored as per the customer's internal policies.

Data backup protection: backups are kept as per the customer's internal policies.

APV Display Client:

Due to the nature of the application it is designed and deployed as a stand-alone application. Health check are put into place to restart the application in case it fails. This is achieved by installing a background process called "DDC Manager" that constantly checks if the Display client application is running and restarts it if it has stopped.

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:

APV is deployed using **SITA managed on-premises hosted**:

No cloud involved for on-premises installations.

APV is deployed using **Customer managed hosted**:

No cloud involved for on-premises installations.

APV Display Client:

No cloud involved for on-premises installations.

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)