Security Technical and Organizational Measures (TOM) Appendix for SITA Airport Vision Evolved (APVe) service schedule

Version: January 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:

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.

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.

NIDS: means Network Intrusion Detection System is a system that attempts to detect hacking activities, denial of service attacks or port scans on a computer network or a computer itself. The NIDS monitors network traffic and helps to detect these malicious activities by identifying suspicious patterns in the incoming packets.

NIPS: means Network Prevention System is a system that protects networks from cyber attacks. These systems constantly monitor networks for threats and automatically take action (such as blocking traffic, killing processes, or quarantining files) when one is detected.

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.

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 APVe service.

TLS: means Transport Layer Security which is a cryptographic protocol that provides end-to-end security of data sent between applications over a network.

K8s: means open-source container orchestration system designed to automate the deployment, scaling, and management of containerized applications.

Velero: means an open source tool to safely backup and restore, perform disaster recovery, and migrate Kubernetes cluster resources and persistent volumes.

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. APVe specific security measures

The below security measures are implemented at APVe level. APVe consists of APVe web client and APVe Display Client.

3.2.1. Network security

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

APVe is deployed using SITA managed Azure cloud hosted:

- Network segmentation: micro-segmentation is implemented through Azure network security groups
- Web application firewall: a network based WAF is implemented
- Firewall: server-based firewalls are implemented
  - Intrusion Prevention Systems: network-based intrusion prevention systems (NIPS) are implemented based on firewalls having these capabilities
  - Intrusion Detection Systems: network-based intrusion detection systems (NIDS) are implemented based on firewalls having these capabilities
- Network devices hardening: TLS 1.2 and above is implemented, and robust password policies are enforced;
- Azure hardening standards are in place
- OIDC authentication: OIDC Authentication relies on ID tokens.

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:

APVe is deployed using SITA managed Azure cloud hosted:

- Antivirus: antivirus is deployed on servers
- Vulnerability management: a vulnerability management process is documented and implemented:
  - Penetration tests are performed at least once year
- Patch management: CI/CD process is implemented:
  - As CI/CD is followed, patching is not part of the product as isses are detected immediately and normally fixed for the next weekly release
- Change Management: CI/CD process is implemented:
  - As CI/CD is followed. New changes are pushed out weekly in small increments. Documentation is kept about changes to the APIs released every week
- 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: managed by SITA Azure Cloud operations team: logs are centralized within the Azure portal; any personal data stored in these logs is anonymized; Application Insights is used to monitor the Service, with both actions and errors logged; logs audit trail is ensured as they are kept for 3 months, and logs are then automatically deleted once retention time has passed
- Azure NTP is used
- System hardening: system hardening activities are performed based on CIS benchmark.

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:

APVe is deployed using SITA managed Azure cloud hosted:

- Secured information exchange / data in transit encryption: information is exchanged securely using HTTPS (TLS 1.2 or higher)
- No personal data are being processed or stored
- Passwords are encrypted using Salt and Hash
- Information deletion: Default 30 days data retention period is configured but can be customized as per customer need
- 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.

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:

APVe is deployed using SITA managed Azure cloud hosted:

- Authentication: password policy and complexity rules are documented and implemented:
    - A session timeout of 1 hour is in place; the application has a configuration of 3 failed attempts after which the account would be locked indefinately and only the administrator can either unlock or reset the password in case user forgot it
- 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

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:

APVe is deployed using SITA managed Azure cloud hosted:

- Secure coding: a secure coding policy is documented and implemented:
    - 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: JSON Web Token (JWT) is implemented to secure authentication

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:

APVe is deployed using SITA managed Azure cloud 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 encrypted in a dedicated storage on the cloud
- Data backup protection: backups are kept on a separate storage, segregated from production environment
- Database is exported nightly and retained for 30 days
- Database snapshots are regularly taken to allow for more granular backups (if only Database data needs to be restored)
- Media files and K8s configurations are backed up nightly using Velero and retained for 30 days.

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:

APVe is deployed using SITA managed Azure cloud hosted:

- Datacenter access restrictions: standard Microsoft Azure security measures are implemented
- Cloud infrastructure redundancy: Microsoft Azure cloud is deployed across landing zones

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)