Security Technical and Organizational Measures (TOM) Appendix for SITA eVisa/ETA service schedule

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 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.

DRP: means Disaster Recovery Plan which is a formal document created by an organization containing detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyberattacks and any other disruptive events.

GDPR: means General Data Protection Regulation which is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

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.

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 eVisa**/**ETA service.

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.

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

TOMs: means Technical and Organizational Measures is a Data Privacy annex listing security controls aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

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. SITA eVisa/ETA specific security measures

The below security measures are implemented at SITA eVisa**/**ETA level:

3.2.1. Network security

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

- Network segmentation:
    - Firewall segmentation to separate different service tiers such as development, pre-production and production.
    - Segmentation of application functionality to minimise connectivity between messaging activities, data activities and application processing activities.
    - External traffic is terminated outside of the main application service and in a segregated network partition.
- Network Encryption:
    - Data exchanged with customer sites is encrypted based on customer requirements.
- VPN is used to restrict, secure, audit and manage remote access:
    - Remote access to the Service for SITA operations and support staff is via VPN.
    - 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 or 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:

- Vulnerability management: a vulnerability management process is documented and implemented:
    - Continuous runtime vulnerability scans are performed on the running software where required by customers.
    - Software is scanned during the CI/CD process whenever software changes are released.
- Patch management: a patch management process is documented and implemented:

    - A dedicated 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:
    - An ITSM tool is used to track all changes; all non-standard changes go through the CAB process, depending on customer policies.
- Capacity management:
    - Monitoring and supervision tools are used to assess and alert on any capacity issues on network devices and servers (CPU, memory utilization, resource utilization).
    - Traffic loads are recorded and monitored for the purpose of capacity planning.
    - 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. The logs are rotated weekly and retained for four weeks. Logs are automatically deleted when the four weeks retention period ends.
- 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 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 outside into and out of the Servive.
- Information is deleted depending on customer data retention policies.

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:

- All access to the Service is governed by strong authentication and authorisation policies.
- 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/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 depending on customer policies.
- Data backup protection: backups segregated from production environment, backup data is encrypted.Disaster recovery plan: DRP test policy, process and procedure, business impact analysis, degraded mode, alternative solutions.
- Disaster recovery testing is tested at least once a year: DRP test policy, process and procedure, regular testing.

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)