Security Technical and Organizational Measures (TOM) Appendix for SITATEX IP service schedule

Version: January 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 (SITATEX IP), its optional features (SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK') and SITATEX Server (only accessible to SITA and hosted in ATI Cloud).

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.

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.

CWE: means Common Weakness Enumeration which is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

DevOps: means a set of practices that combines software development (Dev) and IT operations (Ops). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.

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 Virtual Private Network which is a networking technology that allows users to connect to their main network remotely, using MPLS technology to prioritize internet traffic and avoid public gateway to increase security.

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.

QA: means Quality Assurance which is the environment in which tests are performed to ensure that the software complies with minimum quality requirements, before being deployed into production.

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 SITATEX IP service.

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. SITATEX IP specific security measures

The below security measures are implemented at SITATEX IP level:

3.2.1. Network security

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

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

As the Service and its optional features are deployed on-premises and managed by the Customer, network security (network segmentation, firewall, IDS/IPS, VPN, network device hardening, network authentication) falls under the Customer's responsibility. Should Customer provide an external access to their network for SITA support purpose, the security measures implemented in that case are not under SITA's responsibility.

SITATEX Server (ATI Cloud):

- Network segmentation: all SITA Messaging products hosted in SITA ATI Cloud are segregated from other SITA networks. This limits the exposure of core Messaging systems for an external attacker. Filtering is also applied to ensure Customers are segregated on Messaging network,
- Firewall: server-based firewalls performing filtering based on source/destination IP/ports are in place; a firewall rule recertification process is defined and followed,
- A VPN is used by SITA personnel, including system administrators, to access any SITA internal network, including the Service internal network, with MFA required,
- Customers can access the Service via an IPVPN to connect to the SITA private IP network,
- Network devices hardening: network devices are hardened based on OVA files from the vendors,
- Network authentication: administration on the network equipment is performed via dedicated administrative interfaces on each device. The network access granting mechanism to these interfaces is handled by TACACS+ protocol.

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:

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

As the Service and its optional features are deployed on-premises and managed by the Customer, operational security (antivirus, system patch management, system change management, infrastructure vulnerability management, capacity management, logging and monitoring, system hardening and system operating, logs retention and deletion procedures) falls under Customer's responsibility.

The below specific operational security measures are however implemented for the Service:

- Application vulnerability management: it is managed as part of the application build pipeline and for each release:
    - SAST, DAST and/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE 25) and to ensure a secure coding.
    - Post-release security testing is also performed by QA teams, with additional scans and ad-hoc penetration testing.
- Application patch management: an application patch management process is properly documented and implemented. When a bug is to be resolved, different actions are launched to resolve it depending on the severity: either a complete build is sent to the Customer, or it is considered and resolved in the next product release.
- Software operating procedures: software operating procedures are documented, and this includes vulnerability management procedures.
- Change management: as changes concern system infrastructure, it falls under Customers' responsibility. However, SITA SGS teams might be involved in supporting Customers in implementing some changes.
- Logging and monitoring: Customers are responsible for managing application logs on their perimeter. They can provide logs extracts to SITA for troubleshooting or investigation purpose. In that case, secure logs transmission requirements remain under Customers' responsibility.

SITATEX Server (ATI Cloud):

- Antivirus: antivirus solutions are installed on all Windows systems,
- Vulnerability management: a vulnerability management policy is documented and implemented. SITA infrastructure management team is monitoring for newly discovered and publicly disclosed vulnerabilities by subscribing to several platforms/forums. Information on vulnerabilities may also come from the SITA information security team,
- Patch management: a patch management policy is documented and implemented:
    - A dedicated team is in place for patch management activities, with notice from SITA information security team on the patches to be enforced,
    - All security patches are tested and certified in a test environment before being deployed in production,
    - Patch approval goes through a CAB process,
    - All patching activities are tracked in SITA ITSM tool,
- A change management procedure is documented and implemented:
    - Both infrastructure and software changes/updates are only performed by authorized personnel who have been properly trained,
    - An ITSM tool is used to track all software change requests,
    - All non-standard changes go through a 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 on-premises components (CPU, memory utilization, resource utilization),
- System operating procedures: standard operating procedures are documented,
- Logging and monitoring:
    - Network components logs are collected and centrally stored into SITA' SIEM,
    - All systems use the NTP protocol to synchronize their clocks,

- The content of messages going through SITATEX Server is logged. Any credit card information that can appear in these logs is anonymized. These logs are retained in local files for 24 hours and are then transferred to an internal repository for archiving.
- Systems logs are retained on SITATEX Server for 30 days and are then transferred to an internal repository for archiving.

- System hardening: VMs are hardened based on dedicated template, developed by SITA infrastructure management team.

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; 08.15. 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:

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

As the Service and its optional features are deployed on-premises and managed by the Customer, information protection (data classification, data labelling, data desensitization, data at rest encryption, data deletion) falls under Customer's responsibility.

SITATEX Server (ATI Cloud):

- Data classification: all messages are considered as confidential as potentially containing personal data,
- Data desensitization: SITA does not use any real data as part of its development process,
- Data at rest encryption: all messages are stored encrypted,
- Secured information exchange: Customers can choose to connect to SITA's network through a dedicated IPVPN or through internet, in any case communications are encrypted:
  - In case of internet connection method, communications are performed in HTTPS and are hence encrypted with TLS 1,
  - In case of IPVPN connection method, the data transmitted into the VPN tunnel is encrypted,
- Information deletion: a data retention policy is implemented:
  - Message data:
    - It is retained in SITATEX Server database for a period of 10 days after delivery,
    - SITA shall delete all message data without further notice to Customer within 10 days following the end of the 10-day retention period using a dedicated database script.
  - Logs data:
    - Message logs are retained in the SITATEX Server for a period of 24 hours. These logs are then automatically transferred to an internal log repository for archiving, once the 24 hours retention period is reached,
    - Systems logs are retained in the SITATEX Server for a period of 30 days. These logs are then automatically transferred to an internal log repository for archiving, once the 30 days retention period is reached.

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:

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

As the Service and its optional features are deployed on-premises and managed by the Customer, access control and authentication (secured authentication, conditional access, protection of authentication information, access management, privileged access management) falls under Customer's responsibility.

The below specific information protection measures are however implemented for the Service:

- Authentication: all Customers' connections to Messaging environment are performed through an authenticated and encrypted connection, with appropriate network level filtering in place,
- Protection of authentication information: a feature is implemented in the application, with a pop-up dialog recommending Customers to change default password, even though it remains under their responsibility to do it.
- Restricted access to source code: access to source code is restricted based on RBAC model and least privilege,

SITATEX Server (ATI Cloud):

- Authentication: only SITA personnel can access SITATEX Server. This is performed using a jump server with MFA enabled. SITA password policy is being followed.
- Multi-factor authentication:
    - an MFA is required for SITA personnel login to dedicated jump server to access SITATEX Server,
    - an MFA is required for SITA personnel using VPN to access the Service internal network,
- Protection of authentication information: passwords are stored hashed,
- Restricted access to source code: Azure DevOps Pipelines is used with restricted access to source code implemented based on RBAC model. Only authorized users can access to it,
- Access Management: a process for registering and deregistering SITA users to SITATEX Server is implemented and managed by SITA development team,
- Privileged Access Management: remote access to resources by support and operations teams is performed securely using an encrypted connection (SSH) and a jump server; all privileged accounts actions are logged.

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:

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

- Secure coding: software development follows secure coding guidelines as listed in SITA Secure Coding Checklist. In addition, multiple secure coding controls are in place:
    - No real data is used in the development process,

- Segregation of development and testing environments (hosted in SITA) and the production environment (hosted in Customers' premises),
- A Change Approval Board (CAB) is a mandatory test to validate the product design,
- Security scans are performed with SAST, DAST and/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25).

- Application vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle in the QA environment.
- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions and RBAC model implemented,

SITATEX Server (ATI Cloud):

- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions and RBAC model 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:

SITATEX IP, SITATEX IP Resiliency and SITATEX IP Message Daemon 'SDK' (On-premises – customer managed):

As the Service and its optional features are deployed on-premises and managed by the Customer, service resilience (data backup, data backup protection, systems redundancy, disaster recovery plan, crisis management) falls under Customer's responsibility.

SITATEX Server (ATI Cloud):

- Systems redundancy: infrastructure redundancy is in place enforced through Active/Passive failover. This aims to ensure high availability of SITATEX Server.
- 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	08.13. Information backup; 08.14 Redundancy of information processing activities
Related GDPR principles	Storage limitation; Integrity and confidentiality (security)

3.2.7. Cloud security

The below cloud security measures are implemented for the Service:

SITATEX Server (ATI Cloud):

- Datacenter access restriction: a cloud security policy is in place with strict restrictions implemented:
  - Access control lists that define what resources users are permitted to access; closed circuit video equipment coverage at the facility perimeter at all access control points; security camera monitoring; facility-based security video data recorded and retained for at least 90 days; datacenter access restricted with MFA; 24x7x365 onsite security staff providing additional protection against unauthorized entry; audit trails, log collection and monitoring; regular physical security independent audits.

- Cloud infrastructure redundancy: SITA ATI Cloud infrastructure includes compute, network, storage and management plane redundancies, to ensure resiliency and high availability.
- Cloud backup recovery testing: a dedicated solution is used to perform data backups of critical datacenter management systems and to monitor the backups for completion status; backups are stored offsite via cloud infrastructure managed through the dedicated solution; on a daily basis, a report evidencing the success or failure of each scheduled backup is generated.

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)