

# Security Technical and Organizational Measures (TOM) Appendix for SITA Type B Distribution service schedule

Version: January 2024

## 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 inconsistency 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.

**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.

**MATIP:** means Mapping of Airline Traffic over Internet Protocol which is a communication protocol created for the use by computer applications to carry airline reservation, ticketing, and messaging traffic.

**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.

**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.

**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.

**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 SITA Type B Distribution 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.

**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. SITA Type B Distribution Service specific security measures

The below security measures are implemented at SITA Type B Distribution Service level:

##### 3.2.1. Network security

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

- Network segmentation: network segmentation is implemented, and the service is not exposed to internet except for machine-to-machine connections:
  - SITA Type B Distribution Service is located in Messaging virtual data center regrouping SITA Messaging products having inter-dependencies; network segmentation is implemented within Messaging VDC to segregate it from the Internet and the DC network;
- Firewall: network-based firewalls are implemented both for internal traffic and external traffic with a filter on the outbound connections based on source, destination IP and ports;
- IPS: Network-based and Host-based Intrusion Prevention System are implemented;
- IIDS: Network-based and Host-based Intrusion Detection system are implemented;
- VPN: a remote access for support and operation teams is implemented via SITA Corporate VPN with multifactor authentication;
- Network devices hardening: Hardened OVA file from the vendors are deployed and network devices authentication relies on TACACS+ protocol;
- Network authentication: network authentication relies on protocols such as Radius and SAML;

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:

- Patch management: a dedicated patch management procedure is documented and implemented:
  - Patches are gathered from different sources with service level agreement based on their severity and are systematically tested before implementation in 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 Change Approval Board (CAB) process;
- Capacity management: a capacity management process is documented and implemented:
  - A dedicated application is used to assess and alert on any capacity issues on the service resources (CPU, memory utilization, resource utilization);

- System operating procedures: standard system operating procedures are documented;
- Logging and monitoring: application, infrastructure and system events are captured (e.g., log in/off, successful and unsuccessful login attempts) and stored out of production environment;
  - All system clocks are synchronized with an approved time source;
- System hardening: all systems are built with a hardened image based on CIS hardening benchmark; new servers go under a hardening phase with automated scripts;

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:

- Data classification: all customer data (i.e., messages) are classified as confidential;
- Secured information exchange / data in transition encryption: all external communications are encrypted;
  - Either via SSL/TLS 1.2, via IPVPN or MATIP across SITA Private network;
- Data deletion: a data retention policy is implemented with a retention period of 13 months including contents of type B messages once they are delivered to clients;
  - Once the retention period is reached, data is deleted via daily automated script;

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:

- Authentication: only SITA has access to the service and a password policy is documented and implemented;
- Protection of authentication information: passwords of the service administration console are stored encrypted;
- Restricted access to source code: access to source code is restricted to SITA authorized users;
- Privileged Access Management (PAM): a RBAC model is implemented with one role (i.e., the service does not provide any user interface for customers), and a secured connection is enforced for SITA authorized users;
  - In addition to SITA Corporate VPN with multifactor authentication, SITA authorized users access to the service resource via a secure encrypted connection (SSH) and a jump server; connection to the service administration console is encrypted via HTTPS TLS 1.2;
- Access management: an access management process is implemented with two dedicated teams – one for access provisioning and one for access ordering – and based on an ITSM tool;
- Segregation of duties (SoD): a SoD policy is implemented for the service and for customer account management;
  - Ordering and provisioning teams have different duties, as well have operations and development teams;

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: a secure coding policy is documented and implemented:
  - It is shared by SITA information security team and followed by developers; some peer code reviews are performed within the development teams; SAST, DAST and/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10) and to ensure a secure coding;
- Secure CI/CD platform: a privately hosted platform is used, with VPN required to connect to it;

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:

- Systems redundancy: infrastructure redundancy is in place through clustered services (Active-Standby) to ensure high availability:
  - Two databases per data center are populated synchronously and both are replicated in standby database;
- 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 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:

- 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 is a highly redundant infrastructure including compute, network redundancy, storage and management plane redundancies, and ensuring 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 with a retention period of 7 days managed through the dedicated solution; on a daily basis, a report evidencing the success or failure of each scheduled backup is generated; Recovery Time Objective (RTO) is set to 24 hours; Recovery Point Objective (RPO) is set to 24 hours;

<b>References</b>	
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)