

Security Technical and Organizational Measures (TOM) Appendix for SITA EDI Services

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.

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.

CPU: means Central Processing Unit which is the component of a computer system that controls the interpretation and execution of instructions.

Data anonymization: means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject, and no additional information can restore the original information.

Data pseudonymization: means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

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.

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).

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.

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.

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

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.

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.

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.

Service: means SITA X.400 Messaging service.

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.

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.

VM: means Virtual Machine which is a software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.

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 X.400 Messaging specific security measures

The below security measures are implemented at SITA X.400 Messaging level:

3.2.1. Network security

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

- 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 is in place; a firewall rule recertification process is defined and followed,
- Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS): IPS and IDS are implemented on all network paths and aim to scan network flows for malwares and viruses. File integrity checks are also performed on all gateway,
- A VPN is used by SITA personnel, including system administrators, to access any SITA internal network, including the Service internal network, with MFA enforced,
- 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:

- Vulnerability management: a vulnerability management policy is documented and implemented:
 - o 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,
 - o Various vulnerability scans using dedicated scanning tools are regularly performed on the Messaging environments and SITA assets: monthly scans on the internet-facing SITA assets and ad-hoc scans every 60 to 90 days in the Messaging QA and Production environments,
- 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:
 - 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),
- Logging and monitoring:
 - Network components logs are collected and centrally stored into SITA's SIEM,
 - Application logs are collected and stored into an internal log repository,
 - All systems use the NTP protocol to synchronize their clocks,
- 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; 08.08. 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 messages are considered as confidential as potentially containing personal data,
- Information deletion: a data retention policy is implemented:
 - Message data is retained up to 48 hours in the services in case it is not delivered; after 48 hours, message is deleted through an automatic process.
 - Logs data:
 - It is retained in the Service for a period of 10 days and then is deleted,
 - Logs data is automatically transferred to an internal log repository for archiving.

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 personnel is able to access the Service console:
 - o For SITA authentication to the Service administration interface, the authentication mechanism is based on the use of a jump server with a login and a password. A password policy is implemented, which enforces strong password rules,
- Multi-factor authentication: an MFA is required for SITA personnel using VPN to access the Service internal network,
- Restricted access to source code: the Service is based on a commercial solution; restricted access to source code is managed by the vendor
- Privileged Access Management: an RBAC model is implemented with a dedicated Administrator role; 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,
- Segregation of Duties: SoD is enforced using RBAC model, and with different teams involved in the process (provisioning, development, operations and ordering teams). SoD is managed at Messaging portfolio level.

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: the Service is based on a commercial solution; vendor secure coding practices are implemented;
- Vulnerability scanning: monthly vulnerability scans are launched in production and non-production environments;

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

3.2.6. Service resilience

The below specific service resilience security measures are implemented for the Service:

- 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	08.14. 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.

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)