Security Technical and Organizational Measures (TOM) Appendix for SITA Connect service schedule

APPENDIX 2 FOR ANNEX A OF DATA PROTECTION AGREEMENT

Version: November 2022

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:

AD: means Active Directory which is a Microsoft directory service used for the management of identities' permissions and network access.

AES: means Advanced Encryption Standard which is a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

API: means Application Programming Interface which is a set of programming code that enables data transmission between one software product and another.

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.

Data center: means a centralized physical facility where corporate computers, network, storage, and other IT equipment that support business operations are located providing business-critical applications, services and 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.

Gateway: means a node that provides connection to different networks; for SD-WAN, Gateways allows communication between different regions

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).

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.

IDM: means SITA Identity Management which maintains user information and role associations to so that SITA applications can do role-based access control (RBAC).

IdP: means Identity Provider which is a service that stores and manages digital identities. Companies use these services to allow their employees or users to Connect with the resources they need.

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.

LDAP: means Lightweight Directory Access Protocol which is an open and cross platform protocol used for directory services authentication. LDAP provides the communication language that applications use to communicate with other directory services servers.

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.

NFV: means network function virtualization. It allows virtualization of network services like Firewall, DNS, or WAN acceleration. NFV brings agility to deploy virtual network features 'on demand'

OAuth 2.0 is an industry-standard protocol for authorization.

Radius: means Remote Authentication Dial-In User Service which is an authentication, authorization, and accounting protocol that manages network access.

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.

SDN: means software-defined networking. It is a network architecture that brings to networks what the cloud brought to data centres: automation, virtualization, and orchestration. The control plane (network intelligence) is moved out

from routers & switches to central controllers that manage network layer (SDWAN) and value-added network services (via NFV).

SDWAN: means software-defined wide-area network; a specific application of SDN technology to WAN Connections, which are used to Connect enterprise networks – including branch offices and data centers – over large geographic distances. A key application of SDWAN is to allow companies to build high-performance WANs using available access medias (MPLS, Internet).

SDWAN overlay: means software orchestrated virtual network that is built on top of an underlaying network infrastructure.

SDWAN underlay: means a physical network infrastructure such as MPLS, internet or wireless, that delivers packets across the network.

Service: means SITA Connect 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.

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.

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.

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.

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 CONNECT specific security measures

The below security measures are implemented at SITA Connect level:

3.2.1. Network security

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

- Network segmentation: VLAN segmentation
- Zone-based firewalls on routers
- Access Control lists applied on network devices
- Remote access VPN for remote support teams
- Network devices hardening: enabling of secure access through SSH or TLS, disabling of unnecessary services and protocols, enforcement secure access to the console, enforcement of robust password policies, control of access lists for remote administration, restrict physical access to routers and switches, back up configurations, test security configurations
- Network authentication: using protocols such as: Oauth2, TACACS+, RADIUS, LDAP/AD
- SDN segmentation and SD-WAN underlay/overlay separation

The below specific network security measures are additional for SITA Connect GO and SITA Connect GO at airports SDWAN overlay:

- Firewall: Next-Gen firewall at data centers and gateways
- Intrusion Prevention Systems: network-based intrusion prevention system (NIPS) at data centers
- Intrusion Detection Systems: network-based intrusion detection systems (NIDS) at data centers

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: vulnerability management policy, process and procedure, vulnerability scanning, penetration testing
- Patch management: patch management policy, process, and procedure
- Change management: change management policy, process and procedure, use of an ITSM tool, change acceptance board (CAB)
- Capacity management: capacity management policy, process and procedure

- System operating procedures
- Logging and monitoring: product logs collection and protection, logs analysis through a SIEM for system security monitoring;, logs retention period is set to 367 days, with automated deletion as soon as the 367 days retention period is reached
- System hardening: system hardening policy, process, and procedure, hardening at asset installation, regular application of hardening baseline

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:

- Data in transit encryption: all communications over MPLS and Internet connectivity and intra data centers when transiting over untrusted networks are secured over encrypted tunnels using industry standard accepted protocols (HTTPS, TLS 1.2) and industry standard encryption mechanism (AES-256)
- Sensitive data encryption at rest: personal data eventually collected for the purpose of allowing customer access to internal service or application portal are encrypted following industry standards and data hold is kept at minim necessary to allow access to the services. Retention period settings are customized at customer level.

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:

- Strong authentication for privileged access to devices & portals: password policy, enforcement of password complexity rules, account sessions management with account locker, log out time
- Segregation of duties for SITA Privileged Users accessing the system remotely (SoD): SoD policy, process and procedure, SoD matrix, account creation and access rights validation process ensuring SoD
- Unique account per SITA Privileged User

The below specific network security measures are additional for SITA Connect GO and SITA Connect GO at airports SDWAN overlay:

- Optional Integration of customer IdP solution for access to SD-WAN overlay portal
- MFA for access to SD-WAN overlay components

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
- Vulnerability scanning: regular exposed assets vulnerability scanning
- Penetration testing: regular exposed assets penetration testing
- Secure CI/CD platform

The below specific network security measures are additional for SITA Connect GO and SITA Connect GO at airports SDWAN overlay:

- API security: OAuth2-based API security for SD-WAN Overlay backend communications

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 backup policy, process and procedure are customized at platform and customer level(,customization

Systems redundancy: Active/Active or Active/Standby topologies; setup is customized based on customer and project requirements(**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:

- Data center access restriction: cloud security policy, data center physical access monitoring, badging system, badging systems logs collection and review, CCTV

Cloud redundancy capabilities: hardware redundancy, geographic redundancy

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)