Security Technical and Organizational Measures (TOM) Appendix for SITA Smart Path Bag Drop – SITA SBD Application Service Schedule

Version: November 2025

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 (TOMs) 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 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:

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.

CAB: means Change Advisory Board which is the managerial instance supporting the assessment, prioritization, authorization, and scheduling of changes.

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 Delivery 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.

Service: means SITA Smart Path Bag Drop - SBD Application service.

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.

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.

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.

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.

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.

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.

TDE: means Transparent Data Encryption which is a technology used to encrypt database files at the file level, ensuring that data at rest is protected

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.

AWS GuardDuty: means a threat detection service that continuously monitors and analyses AWS data sources and logs to identify suspicious and potentially malicious activity in your AWS environment.

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

3. Security Technical and Operational 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 document.

3.2. SITA SBD Application specific security measures

The below security measures are implemented at SITA SBD Application Service level.

3.2.1. Network security

SBD Business Logic (BL) Server deployed using **SITA managed Azure cloud hosted** option:

- Network segmentation: micro-segmentation is implemented through Azure network security groups,
- Network devices hardening: TLS 1.2 and above is implemented, and robust password policies are enforced; Azure hardening standards are in place,
- Network authentication: network authentication relies on protocols such as Kerberos and LDAP/Active Directory.

SBD BL Server deployed using **SITA managed AWS cloud hosted** option:

- Network segmentation: micro-segmentation is implemented through AWS security groups,
- Network devices hardening: TLS 1.2 and above is implemented, and robust password policies are enforced; AWS hardening standards are in place,
- Network authentication: network authentication relies on protocols such as Kerberos and LDAP/Active Directory.

If SBD Application frontend is deployed using **SITA managed** option:

- Network segmentation: VLAN segmentation, Firewall segmentation is implemented at airport.

If **SBD Application** frontend is deployed using **Customer managed** option:

- In case of deployment managed by the Customer, network security 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.

If **Bag Drop BHS Gateway** is deployed using **Customer managed** option:

- In case of deployment managed by the Customer, network security 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.

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:

SBD BL Server deployed using **SITA managed Azure or AWS cloud hosted** option:

- Vulnerability management: a vulnerability management process is documented and implemented:
  - Penetration tests are performed at least once year.
- Patch management: a patch management process is documented and implemented:
  - Patch management activities are managed using Azure Patch Manager / AWS Systems Manager Patch Manager (Update Management) tool.
- 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.
- 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 network devices and servers (CPU, memory utilization, resource utilization)
- System operating procedures: standard operating procedures are documented.
- Logging and monitoring:
  - Azure: Logging and monitoring are managed by Azure Application Insights; logs are centralized within the Azure portal.
  - AWS: Logging and monitoring are managed by AWS CloudWatch; logs are centralized within the AWS portal.
  - If any personal data stored in these logs, it is anonymized.
  - Log audit trail is ensured as they are kept for 3 months, and logs are then automatically deleted once retention time has passed.
  - Logs and reports can also be accessed via an application callled “DataManager”. Any personal data is anonymized here, as well. The retention time is 3 months as well.
- Azure / AWS NTP is used.
- System hardening: system hardening activities are performed based on CIS benchmark and Azure defender / AWS GuardDuty.

If SBD Application (Frontend) is deployed using **SITA managed** option:

- Patch management: a patch management process is documented and implemented:
  - A dedicated team is in place and relies on industrialized patching tools; 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.
- System operating procedures: standard operating procedures are documented.

- System hardening: a system hardening policy and checklist is documented and implemented:
    - Workstation is hardened based on CIS benchmark.

If SBD Application (Frontend) is deployed using **Customer managed** option:

- Patch management / change management: application patch and change management follows SITA standard documented processes and procedure:
    - An ITSM tool is used to track all application changes and patches, which all go through the CAB process, except for standard changes.
    - System patch management remains under Customer's responsibility.
- Antivirus, vulnerability management, capacity management, logging and monitoring, system hardening, system operating procedures: in case of on-premises deployment managed by Customer, those security controls are Customer's responsibility.

If Bag Drop BHS Gateway is deployed using **Customer managed** option:

- Same as Bag Drop Application (BDA) when it is deployed using Customer managed option.

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:

SBD BL Server:

- Data at rest encryption (Database TDE encryption)
- Data in transit encryption / secure information exchange: personal data communication is encrypted using HTTPS (TLS 1.2 or above)
- Information deletion: a data retention policy is documented and implemented:
    - No personal identifiable information (PII) is stored permanently in the product.
    - All PII required for passenger processing is retained in a cache for 5 minutes unless DCS Host integration requires otherwise.
    - All troubleshooting logs are retained for 90 days by default.
    - SITA shall delete all data without further notice to the customer following the end of the configured data retention period; an automatic dedicated job is launched as soon as the data retention period has passed.

SBD Application (Frontend):

- No personal identifiable information (PII) is stored permanently in the client by default.
- Troubleshooting logs are kept for 60 days by default.
- Data desensitization: Logs are anonymized by default.

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:

SBD BL Server

- Authentication:
  - HTTPS is used for authentication the communication between the SBD Application Frontend and the Backend.
  - Protection of authentication information: all passwords are stored encrypted.
- Multi-factor authentication (MFA): MFA is implemented to ensure restricted access to source code and in addition to the VPN, for remote administration and support by SITA administrators.
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC model and based on MFA implementation.
- Segregation of duties (SoD): SoD is implemented using RBAC model: several roles and account types are used to respect the principle of least privilege.

SBD Application (Frontend):

- Uses SBD-BL Server provided authentication.
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC model and based on MFA implementation.

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:

SBD BL Server, Bag Drop BHS Gateway, and SBD Application (Frontend):

- Secure coding: a secure coding policy is documented and implemented:
  - It is shared by SITA information security team and followed by developers; a secure coding checklist is used including scans.
  - A DevOps guide is provided to the developers and describes a list of best practices regarding secure coding, data protection and security development measures.
  - SAST, DAST and/or SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25) including open-source libraries.
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle before each code release.

- Secure CI/CD platform: Jenkins Build Pipelines is used, with restricted permissions on who can run the pipeline and promote the code; deployment requires an approval process.

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:

SBD BL Server:

- Data availability: RTO and RPO are documented and agreed upon within agreements with Customers.
- Data backup: a data backup policy is documented and implemented:
  - Databases are backed up **every 24 hours (per default, can be agreed differently with customer).**
  - The data backup retention time is **1 week (per default, can be agreed differently with customer).**
  - SITA shall delete all data backup without further notice to Customer following the end of the configured backup data retention period.
- Data backup protection: backups are segregated from the production environment; backups are encrypted.
- Systems redundancy: application redundancy is in place through clustered services to ensure high availability as per agreed SLA.

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

SBD BL Server:

- Datacenter access restrictions: standard Microsoft Azure / Amazon AWS security measures are implemented.
- Azure Advisor security baseline / AWS Trusted Advisor checks is used, and recommendations followed and implemented.
- Cloud redundancy capabilities: hardware redundancy and geographic redundancy as per agreed SLA.

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)