Security Technical and Organizational Measures (TOM) Appendix for Bag Manager service schedule

Version: December 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 (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:

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 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.

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.

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.

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.

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.

Transparent Data Encryption: means encryption of database at file level to secure data at rest.

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 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 TOM.

3.2. Bag Manager specific security measures

The below security measures are implemented at Bag Manager level. Bag Manager consists of Bag Manager client and Bag Manager Depot.

3.2.1. Network security

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

If **Bag Manager V6** is deployed using **On-premises (SITA managed) hosted** option:

- Network segmentation: VLAN and firewall segmentation is implemented to isolate sensitive components,
- Firewall: software-based and network-based firewalls are implemented,
- Network devices hardening: SSH is enabled with TLS 1.2; hardening measures are implemented; scans are regularly launched to verify hardening compliance.

If **Bag Manager V6** is deployed using **SITA managed Azure Cloud hosted** option:

- Network segmentation: micro-segmentation is implemented through Azure network security groups,
- Web application firewall: a network based WAF is implemented,
- Firewall: server-based firewalls are implemented,
    - Intrusion Prevention Systems: network-based intrusion prevention systems (NIPS) are implemented based on firewalls having these capabilities,
    - Intrusion Detection Systems: network-based intrusion detection systems (NIDS) are implemented based on firewalls having these capabilities,
- Network devices hardening: TLS 1.2 (or higher) 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

If **Bag Manager V7** is deployed using **SITA managed Azure Cloud hosted** option:

- Network segmentation: micro-segmentation is implemented through Azure network security groups,
- Web application firewall: a network based WAF is implemented,
- Firewall: server-based firewalls are implemented,
    - Intrusion Prevention Systems (IPS): network-based intrusion prevention systems (NIPS) are implemented based on firewalls having these capabilities,

- Intrusion Detection Systems (IDS): network-based intrusion detection systems (NIDS) are implemented based on firewalls having these capabilities,

- Network devices hardening: TLS 1.2 (or higher) 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

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:

<u>If Bag Manager V6 is deployed using On-premises (SITA managed) hosted option:</u>

- Antivirus: an antivirus is deployed on workstations,
- Vulnerability management: a vulnerability management process is documented and implemented:
  - Penetration tests are performed at least once year in pre-prod environment,
- Patch management: a patch management procedure is documented and implemented:
  - Manual patching is enforced; all patches are tested before moving to UAT or 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 CAB process,
- Capacity management: a capacity management process is documented and implemented:
  - Monitoring tools (scripts) 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 for administration and support, including standard security configurations,
- Logging and monitoring: all users access and systems logs are collected on both infrastructure and applicative levels; firewall security logs are analysed in a SIEM; some manual logs reviews are also performed on an ad-hoc basis in case of incident or troubleshooting; logs are retained for a week before being archived,
- System hardening: pre-hardened deployment are performed based on SITA Baggage hardening catalog, itself based on CIS Benchmark.
- **If Mobile solution is included,** Device management: a device management process is documented and implemented:
  - A Mobile Device Management (MDM) solution is implemented for software management, scripts deployments, license management and device monitoring,
  - Data in transit to and from the devices are encrypted; no data is stored on the device itself,
  - A safe device disposal process is implemented.

<u>If Bag Manager V6 is deployed using SITA managed Azure Cloud hosted option:</u>

- Antivirus (for clients, for servers Antivirus: antivirus is deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
    - Penetration tests are performed at least once year in pre-prod environment,
- Patch management: a patch management process is documented and implemented:
    - Patch management activities are managed using Azure 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: Logging and monitoring is managed by SITA Azure Cloud operations team: logs are centralized within the Azure portal; any personal data present in these logs is anonymized; Application Insights is used to monitor the Service, with both actions and errors logged; logs audit trail is ensured as they are kept for 3 months, and logs are then automatically deleted once retention time has passed,
- Azure NTP is used;
- System hardening: system hardening activities are performed based on CIS benchmark.
- **If Mobile solution is included**
    - Device management: a device management process is documented and implemented:
    - A Mobile Device Management (MDM) solution is implemented for software management, scripts deployments, license management and device monitoring,
    - Data in transit to and from the devices are encrypted; no data is stored on the device itself,
    - A safe device disposal process is implemented.

<u>If Bag Manager V7 is deployed using SITA managed Azure Cloud hosted option:</u>

- Antivirus (for clients, for servers Antivirus: antivirus is deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
    - Penetration tests are performed at least once year in pre-prod environment,
- Patch management: a patch management process is documented and implemented:
    - Patch management activities are managed using Azure 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: Logging and monitoring is managed by SITA Azure Cloud operations team: logs are centralized within the Azure portal; any personal data present in these logs is anonymized; Application Insights is used to monitor the Service, with both actions and errors logged; logs audit trail is ensured as they are kept for 3 months, and logs are then automatically deleted once retention time has passed,
- Azure NTP is used;

- System hardening: system hardening activities are performed based on CIS benchmark.
- **If Mobile solution is included**
    - Device management: a device management process is documented and implemented:
    - A Mobile Device Management (MDM) solution is implemented for software management, scripts deployments, license management and device monitoring,
    - Data in transit to and from the devices are encrypted; no data is stored on the device itself,
    - A safe device disposal process is implemented.

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:

<u>If Bag Manager V6 is deployed using On-premises (SITA managed) hosted option:</u>

- Data classification: different security requirements to be implemented depending on the data classification level; operational data and user data are segregated in different schemes at database level,
- Secured information exchange / data in transit encryption: information is exchanged securely using HTTPS with signed certificates, SFTP and MQ SSL; AES-256-GCM encryption mechanism is used,
- Data at rest encryption: database encryption is implemented; all personal data are encrypted; all passwords are encrypted with SHA-512.
- Information deletion: default data retention policies are implemented:
    - The retention period goes from 30 to 180 days, configurable based on Customer's requirements. Customer shall specify to SITA the data retention period up to a maximum of 180 days.
    - SITA shall delete all data without further notice to Customer following the end of the configured data retention period.
    - Data delete is automatically performed through a dedicated script as soon as the data retention period is reached. A job is launched on a daily basis and deletes all the reports that expired.
    - A monitoring process is in place to ensure the delete process is properly triggered.

<u>If Bag Manager V6 is deployed using SITA managed Azure Cloud hosted option:</u>

- Data classification: different security requirements to be implemented depending on the data classification level; operational data and user data are segregated in different schemes at database level,
- Secured information exchange / data in transit encryption: information is exchanged securely using HTTPS (TLS 1.2 or higher)
- Data at rest encryption: all personal data are encrypted; all passwords are encrypted with SHA-512.
- Information deletion: default data retention policies are implemented:

- The retention period goes from 30 to 180 days, configurable based on Customer's requirements. Customer shall specify to SITA the data retention period up to a maximum of 180 days.
- SITA shall delete all data without further notice to Customer following the end of the configured data retention period.
- Data delete is automatically performed through a dedicated script as soon as the data retention period is reached. A job is launched on a daily basis and deletes all the reports that expired.

If **Bag Manager V7** is deployed using **SITA managed Azure Cloud hosted** option:

- Data classification: different security requirements to be implemented depending on the data classification level; operational data and user data are segregated in different schemes at database level,
- Secured information exchange / data in transit encryption: information is exchanged securely using HTTPS (TLS 1.2 or above)
- Data at rest encryption: all personal data are encrypted; all passwords are encrypted with Bcrypt.
- Information deletion: default data retention policies are implemented:
  - The retention period goes from 30 to 180 days, configurable based on Customer's requirements. Customer shall specify to SITA the data retention period up to a maximum of 180 days.
  - SITA shall delete all data without further notice to Customer following the end of the configured data retention period.
  - Data delete is automatically performed through a dedicated script as soon as the data retention period is reached. A job is launched on a daily basis and deletes all the reports that expired.

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:

If Bag Manager V6 is deployed using On-premises (SITA managed) hosted option:

- Authentication: password policy and complexity rules are documented and implemented:
  - A session timeout is in place; the application has a configuration for number of failed login attempts after which the account would be locked and only the administrator can reset,
- Restricted access to source code: access to source code is restricted based on the RBAC model implemented.
- Privileged Access Management: SITA applies a "Least Privilege" and "Need to Know" approach.
- Multi-factor authentication: MFA is implemented to ensure restricted access to source code and in addition to the VPN, for remote administration and support by SITA administrators,
- Segregation of duties (SoD): segregation of duties is enforced on SITA side for administrative rights with 2 dedicated user roles (SupAdmin / Admin).

If Bag Manager V6 is deployed using SITA managed Azure Cloud hosted option:

- Authentication: password policy and complexity rules are documented and implemented:
    - A session timeout is in place; the application has a configuration for number of failed login attempts after which the account would be locked and only the administrator can reset,
- Restricted access to source code: access to source code is restricted based on the RBAC model implemented.
- Privileged Access Management: SITA applies a "Least Privilege" and "Need to Know" approach.
- Multi-factor authentication: MFA is implemented to ensure restricted access to source code and in addition to the VPN, for remote administration and support by SITA administrators,
- Segregation of duties (SoD): SoD is implemented using RBAC model: several roles and account types are used to respect the principle of least privilege.

If Bag Manager V7 is deployed using SITA managed Azure Cloud hosted option:

- Authentication: password policy and complexity rules are documented and implemented:
    - A session timeout is in place; the application has a configuration for number of failed login attempts after which the account would be locked and only the administrator can reset,
- Restricted access to source code: access to source code is restricted based on the RBAC model implemented.
- Privileged Access Management: SITA applies a "Least Privilege" and "Need to Know" approach.
- A jump server with VPN is implemented; quarterly access rights review are performed; any account is disabled after 3 months if not used, and deleted after 12 months; all privileged actions are logged, including all privileged access and accounts provisioning and deprovisioning,
- Segregation of duties (SoD): segregation of duties is enforced on SITA side for administrative rights with 2 dedicated user roles (SupAdmin / Admin).

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:

If Bag Manager V6 is deployed:

- Secure coding: a secure coding policy is documented and implemented:
    - 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: a dedicated tool is used for vulnerability scanning against OWASP Top 10 at every release, on a quarterly basis,
- API security: JSON Web Token (JWT) is implemented to secure authentication.

If Bag Manager V7 is deployed:

- Secure coding:
    - 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: Azure DevOps Pipelines is used, with restricted permissions on who can run the pipeline and promote the code; deployment requires an approval process,
- API security: JSON Web Token (JWT) is implemented to secure authentication.

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:

If Bag Manager V6 is deployed using On-premises (SITA managed) hosted option:

- Data backup: data backup policy and processes are documented and implemented:
    - Daily scheduled backups (full backups) are launched; backups are stored in a dedicated storage on the cloud,
    - Data backup retention period depends on the Customers' requirements and is a maximum of 190 days (180 days of retention period with 10 additional days after the end of the retention period). Unless agreed otherwise, SITA shall delete all data backup without further notice to Customer.
- Data backup protection: backups are kept on a separate server, segregated from production environment,
- Systems redundancy: all environments are replicated in an Active/Passive mode, with 15 to 30 minutes required for failover from Active to Passive,
- Disaster recovery plan: If Disaster recovery requirement is agreed in the contract, a standard DRP plan is in place, with the possibility to restore on an alternative environment.
- Disaster recovery testing: the DRP plan is tested on a yearly basis, including backup restoral tests,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

If Bag Manager V6 is deployed using SITA managed Azure Cloud hosted option:

- Data backup: data backup policy and processes are documented and implemented:
    - Daily scheduled backups (full backups) are launched; backups are stored in a dedicated storage on the cloud,
    - Data backup retention period depends on the Customers' requirements and is a maximum of 190 days (180 days of retention period with 10 additional days after the end of the retention period). Unless agreed otherwise, SITA shall delete all data backup without further notice to Customer.
- Data backup protection: backups are kept on a separate storage, segregated from production environment,

- Systems redundancy: all environments are replicated in an Active/Passive mode, with 15 to 30 minutes required for failover from Active to Passive,
- Disaster recovery plan: If Disaster recovery requirement is agreed in the contract, a standard DRP plan is in place, with the possibility to restore on an alternative environment.
- Disaster recovery testing: If implemented, the DR plan is tested on a yearly basis, including backup restoral tests,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

<u>If Bag Manager V7 is deployed using SITA managed Azure Cloud hosted option:</u>

- Data backup: data backup policy and processes are documented and implemented:
    - Daily scheduled backups (full backups) are launched; backups are stored in a dedicated storage on the cloud,
    - Data backup retention period depends on the Customers' requirements and is a maximum of 190 days (180 days of retention period with 10 additional days after the end of the retention period). Unless agreed otherwise, SITA shall delete all data backup without further notice to Customer.
- Data backup protection: backups are kept on a separate storage, segregated from production environment,
- Systems redundancy: all environments are synchronised across multiple availability Zones, with up to 15 minutes required to switch.
- Disaster recovery: If Disaster recovery requirement is agreed in the contract, then:
    - Disaster recovery plan: A standard DRP plan is in place, with the possibility to restore on an alternative environment.
    - Disaster recovery testing: If implemented, the DR plan is tested on a yearly basis, including backup restoral tests.
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.
- redundancy (to meet SLAs)
- Crisis management (crisis management policy, process and procedure, crisis management tooling (e.g., ad hoc communication paths, reflex cards, emergency button)

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 restrictions: Microsoft Azure security measures are applicable.
- Data availability: RTO and RPO are documented and agreed upon within agreements with Customers.

- Cloud infrastructure redundancy: Microsoft Azure cloud is deployed across availability zones.

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)