Security Technical and Organizational Measures (TOM) Appendix for SITA Airport Management (AMS) service schedule

Version: June 2022

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 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

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.

AMS: means the Service.

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

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.

CWE: means Common Weakness Enumeration which is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

DevOps is a set of practices that combines software development (Dev) and IT operations (Ops). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.

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.

DRP: means Disaster Recovery Plan which is a formal document created by an organization containing detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyberattacks and any other disruptive events.

GCM: means Galois/Counter Mode which is a mode used for authenticated encryption with associated data and providing confidentiality and authenticity for the encrypted data and authenticity for the additional authenticated data.

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).

GPO: means Group Policy Object which is an essential component in Microsoft's Active Directory, a GPO defines rules for users, computers, groups and organizational units (OUs). Group Policy Objects are used to establish security settings, install applications, run scripts, set group preferences and configure the Registry.

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.

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.

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

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.

OWASP Top 10: means Open Web Application Security Project Top 10 which 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.

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.

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.

Service: means SITA Airport Management – also known as Airport Management Solution (AMS) – containing both AMS Core v6 and AMS Employee Self Service product modules.

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.

SQL: means Structured Query Language which is a domain-specific language used in programming and designed for managing data held in a relational database management system.

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.

WAF: means Web Application Firewall which is a specific form of application firewall that filters, monitors, and blocks web traffic to and from a web service.

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 Airport Management specific security measures

The below security measures are implemented at SITA Airport Management service level. The service consists of AMS Core v6 and AMS Employee Self Service. The hosting option is to be chosen by the customer – SITA ATI Cloud hosted option OR Azure hosted option OR On-premises (SITA managed) hosted option OR On-premises (Customer managed)]. This schedule applies to the relevant module and option selected by the Customer, as appliable.

3.2.1. Network security

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

AMS Core v6:

SITA ATI Cloud hosted option:

- Network segmentation: firewall segmentation is implemented allowing to segregate between production, preproduction and testing environments, and between Customers endpoints and the AMS backend; VLAN segmentation is also implemented between presentation, applicative and database layers,
- Reverse proxy: a reverse proxy is implemented,
- Firewall: server-based firewalls are implemented both for internal traffic and external traffic,
- 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,
- VPN: a VPN is implemented for remote access allowing SITA support,
- Network devices hardening: TLS 1.2 or above is implemented; robust password policies are enforced; access to physical routers and switches is restricted,
- Network authentication: network authentication relies on protocols such as Kerberos and LDAP/Active Directory.

Azure 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,
- VPN: Azure Gateway is implemented [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE AZURE GATEWAY],

- 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.

On-premises (SITA managed) hosted option:

- Firewall: server-based firewalls are implemented and managed by SITA network team,
- Network devices hardening: hardening activities are performed based on CIS benchmark,
- Network authentication: network authentication relies on protocols such as Kerberos and LDAP/Active Directory.

On-premises (Customer managed) hosted option:

In case of on-premises 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.

AMS Employee Self Service:

- Network protection and segmentation: AMS ESS is a multi-tenant application relying on a single App Service with multiple resource groups configured; inbound traffic is protected through Azure Content Delivery Network and Azure Front Door; outbound traffic to Customers' AMS systems and mail systems is IP-restricted,
- Firewall: firewalls are implemented for the communications between SITA AMS Core v6 and AMS Employee Self Service,
- Network authentication: AMS Employee Self Service relies on Azure AD and a token-based MFA,
- VPN, network devices hardening and additional information on network segmentation: AMS Employee Self Service being hosted in Azure, please refer to Microsoft Product and Services DPA protection addendum – Appendix A – Security measures, available on Microsoft Licensing Resources and Documents webpage.

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:

AMS Core v6:

SITA ATI Cloud hosted option:

- Antivirus: antivirus is deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
  - Environment vulnerability scans are performed; penetration tests are performed at least once a year,
- Patch management: a patch management process is documented and implemented:
  - A dedicated team is in place and relies on industrialized patching tools; all 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,
- 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: unusual login activities such as login from suspicious location outside business hours are logged; manual logs analysis is performed,
- System hardening: a system hardening policy and checklist is documented and implemented:
    - Servers are hardened based on CIS benchmark and configured via GPO. A dedicated tool is used to analyse compliance with the CIS benchmark.

Azure hosted option:

- Antivirus: antivirus is deployed on servers,
- 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 (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: manual logs analysis is performed,
- System hardening: system hardening activities are performed based on CIS benchmark.

On-premises (SITA managed) hosted option:

- Antivirus: antivirus is deployed on servers,
- Vulnerability management: a vulnerability management process is documented and implemented:
    - Environment vulnerability scans are performed twice a year,
- 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,
- 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,
- System hardening: a system hardening policy and checklist is documented and implemented:
    - Servers are hardened based on CIS benchmark and configured via GPO. A dedicated tool is used to analyse compliance with the CIS benchmark.

On-premises (Customer managed) hosted 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.

AMS Employee Self Service:

- Change management: a change management procedure is documented and implemented:
  - A CI/CD process is in place for continuous integration and deployment, with Azure DevOps used to track all the changes to the code. All releases are tested in a staging environment and an approval (CAB) is needed before deployment into production.
  - In operations, an ITSM tool is used to track all changes; all non-standard changes go through the CAB process,
- System operating procedures: standard system operating procedures are documented,
- Logging and monitoring: Azure Log Analytics is used for logging and monitoring purposes; security logs analysis activities are managed directly by Azure as part of the Platform services,
- Antivirus, OS vulnerability management, patch management, capacity management, system hardening: AMS Employee Self Service being hosted in Azure, please refer to Microsoft Product and Services DPA protection addendum – Appendix A – Security measures, available on Microsoft Licensing Resources and Documents webpage.

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:

AMS Core v6:

SITA ATI Cloud hosted option:

- Secured information exchange / data in transit encryption: both ingress and egress traffic are secured through TLS 1.2 encryption with AES-256-GCM cipher,
- Information deletion: Customer data are deleted based on the agreement defined with the Customer, considering the following:
  - In case of agreed data retention period, data purging is automatically performed through a dedicated script as soon as the data retention period is reached. SITA shall delete all data without further notice to Customer within 10 days following the end of the agreed data retention period.
  - In absence of an agreed data retention period, it is limited by the maximum available storage volume. SITA shall delete all data without further notice to Customer within 10 days following the end of the contract.

Azure hosted option:

- Secured information exchange / data in transit encryption: both ingress and egress traffic are secured through TLS 1.2 encryption with AES-256-GCM cipher,
- Data at rest encryption: by default, Azure Disk Encryption is implemented,
- Information deletion: Customer data are deleted based on the agreement defined with the Customer, considering the following:

- In case of agreed data retention period, data purging is automatically performed through a dedicated script as soon as the data retention period is reached. SITA shall delete all data without further notice to Customer within 10 days following the end of the agreed data retention period.
- In absence of an agreed data retention period, it is limited by the maximum available storage volume. SITA shall delete all data without further notice to Customer within 10 days following the end of the contract.

On-premises (SITA managed) hosted option:

- Data at rest encryption: disk encryption is implemented,
- Information deletion: Customer data are deleted based on the agreement defined with the Customer, considering the following:
    - In case of agreed data retention period, data purging is automatically performed through a dedicated script as soon as the data retention period is reached. SITA shall delete all data without further notice to Customer within 10 days following the end of the agreed data retention period.
    - In absence of an agreed data retention period, it is limited by the maximum available storage volume. SITA shall delete all data without further notice to Customer within 10 days following the end of the contract.

On-premises (Customer managed) hosted option:

In case of on-premises deployment managed by the Customer, information protection falls under Customer's responsibility.

AMS Employee Self Service:

- Secured information exchange / data in transit encryption: both ingress and egress traffic are secured through TLS 1.2 or above encryption; connections with SITA AMS Core v6 are restricted to a whitelist of IP addresses,
- Data desensitization: logs are anonymized and only the employee number can be read,
- Data at rest encryption: by default, Azure disk encryption is implemented; Azure Cosmos DB encryption at rest is implemented; Azure Key Vault is used to protect all keys, secrets and certificates,
- Information deletion: Azure Cosmos DB manages the data retention policy, with daily cache clearing,
    - Data is purged automatically by Azure Cosmos DB,
    - SITA shall delete all data without further notice to Customer within 10 days following the end of the configured data retention period,
    - Azure Log Analytics stores logs, with a retention policy of 30 days (by default), and they are then automatically purged.

References	
Related ISO/IEC 27002:2022 controls	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:

AMS Core v6:

SITA ATI Cloud hosted option:

- Authentication: password policy and password complexity rules are documented and implemented:
    - GPO includes account locking capabilities,
- Conditional access: conditional access control is implemented using group policies in Active Directory,

- Single Sign-On (SSO): a Customer SSO service is implemented [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE SSO SERVICE],
- Protection of authentication information: initial account creation is managed by SITA, with mandatory change of password by the user at first login,
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC,
- Privileged Access Management: privilege access roles are identified (Support and Cloud admin team) with limited access based on required privileges; group policies in Active Directory are used,
- Segregation of duties (SoD): SoD is implemented using group policies.

Azure hosted option:

- Authentication: password policy and password complexity rules are documented and implemented:
    - GPO includes account locker capabilities,
- Multi-factor authentication (MFA): MFA is implemented for administration and support accesses,
- Conditional access: conditional access control is implemented using Azure RBAC model,
- Single Sign-On: SSO is implemented at SITA side for support activities; a Customer SSO service is implemented [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE SSO SERVICE],
- Protection of authentication information: authentication is relying on SITA Active Directory,
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC,
- Privileged Access Management: a privileged access management policy is implemented:
    - A bastion is in place and a RBAC model is used,
- Segregation of duties (SoD): SoD is implemented using RBAC model.

On-premises (SITA managed) hosted option:

- Authentication: password policy and password complexity rules are documented and implemented:
    - GPO includes account locking capabilities,
- Conditional access: conditional access controls are implemented using group policies in Active Directory,
- Protection of authentication information: initial account creation is managed by SITA, with mandatory change of password by the user at first login,
- Restricted access to source code: access to source code is restricted based on least privilege principle using RBAC,
- Privileged Access Management: privilege access roles are identified (Support and Cloud admin team) with limited access based on required privileges; group policies in Active Directory are used,
- Segregation of duties (SoD): SoD is implemented using group policies.

On-premises (Customer managed) hosted option:

- Restricted access to source code: restricted access to source code is performed based on RBAC model and least privilege,
- Authentication, multi-factor authentication (MFA), conditional access, Single Sign On (SSO), protection of authentication information, privileged access management (PAM), Segregation of Duties (SoD): in case of on-premises deployment managed by the Customer, those access control and authentication security measures fall under the Customer's responsibility.
    - Should Customer provide an external access to their network for SITA support purpose, the access control and authentication security measures implemented in that case are not under SITA's responsibility.

AMS Employee Self Service:

- Authentication: Azure AD authentication is used; however, the password policy and the password complexity rules remain under the Customer's responsibility,
- Multi-factor authentication (MFA): a token-based MFA using OAuth2 protocol is implemented, [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE MFA]
- Single Sign-On: OpenID Connect (OIDC) protocol against client's identity provider (IdP) is used for SSO purpose, [NOT APPLICABLE IF THE CUSTOMER DOES NOT USE SSO SERVICE]
- Protection of authentication information: authentication is relying on Customers' Active Directory,
- Restricted access to source code: access to source code is restricted based on RBAC model and least privilege,
- Segregation of duties (SoD): SoD is implemented using RBAC model in Azure Pipelines, with different roles to push and approve code.

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:

AMS Core v6:

SITA ATI Cloud option:

- Secure coding: a secure coding policy is documented and implemented:
  - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices,
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle.
- Penetration testing: penetration tests are performed at the application level before each release; some more tests are performed in case of major changes,
- API security: APIs are secured using bearer token-based access.

Azure hosted option:

- Secure coding: a secure coding policy is documented and implemented:
  - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices,
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle.
- Penetration testing: penetration tests are performed at the application level before each release; some more tests are performed in case of major changes,
- Secure CI/CD platform: Azure DevOps Pipelines and Terraform are used, with restricted permissions on who can run the pipeline and promote the code,
- API security: APIs are secured using bearer token-based access.

On-premises (SITA managed) hosted option:

- Secure coding: a secure coding policy is documented and implemented:
  - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices,
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle;
- Penetration testing: penetration tests are performed at the application level before each release,
- API security: APIs are secured using bearer token-based access.

On-premises (Customer managed) hosted option:

- Secure coding: a secure coding policy is documented and implemented:
  - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices,
- Vulnerability scanning: application vulnerability scans are performed as part of software development lifecycle.

AMS Employee Self Service:

- Web application firewall (WAF): A WAF is enabled in preventive mode using Azure Front Door (Azure Content Delivery Network), which provides access to, and management of site content and services deployed by Azure App Services,
- Secure coding: a secure coding policy is documented and implemented:
  - This policy is shared by CISO and followed by developers; there are multiple reviews when code is submitted both at the pull request level and the architecture level; SAST, DAST and SCA tools are used to check against vulnerabilities in the code (OWASP Top 10, CWE Top 25); external development team forms an integral part of the SITA development team and follows similar secure coding practices,
- Vulnerability scanning: vulnerability scans are launched during the development phase before each release,
- Secure CI/CD platform: Azure DevOps Pipelines is used, with restricted permissions on who can run the pipeline and promote the code; automated deployment is implemented,
- API security: APIs are used to reach AMS Core v6 and secured using Azure Front Door and Azure WAF; APIs are secured using bearer token-based access.

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:

AMS Core v6:

SITA ATI Cloud option:

- Data backup: a data backup policy is documented and implemented:
  - Database are backed up through daily full backups and hourly transactional backups,

    - The data backup retention time is 14 days by default for daily full backups (can go up to 30 days on request) and 2 days for transactional backups; servers are backed up daily with 14 days retention period,
    - SITA shall delete all data backup without further notice to Customer within 10 days following the end of the configured backup data retention period,
    - File data is controlled through an automated SQL backup job allowing deletion as soon as the retention is reached; database data is controlled through automated application configuration allowing deletion as soon as the retention is reached,
- Data backup protection: backups are segregated from the production environment,
- Systems redundancy: Active/Passive and Active/Active failovers are in place
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

Azure hosted option:

- Data backup protection: backups are segregated from the production environment; backups are encrypted,
- Systems redundancy: Active/Passive and Active/Active failovers are in place,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

On-premises (SITA managed) hosted option:

- Data backup: a data backup policy is documented and implemented:
    - Database are backed up through daily full backups and hourly transactional backups,
    - The data backup retention time is 14 days by default for daily full backups (can go up to 30 days on request) and 2 days for transactional backups; servers are backed up daily with 14 days retention period,
    - SITA shall delete all data backup without further notice to Customer within 10 days following the end of the configured backup data retention period,
    - File data is controlled through an automated SQL backup job allowing deletion as soon as the retention is reached; database data is controlled through automated application configuration allowing deletion as soon as the retention is reached,
- Data backup protection: backups are segregated from the production environment; backups are encrypted,
- Systems redundancy: Active/Passive and Active/Active failovers are in place depending on the components,
- Disaster recovery testing: a DRP plan is implemented,
- Crisis management: crisis management and major incidents processes are documented and implemented, with dedicated communication paths and escalation process.

On-premises (Customer managed) hosted option:

In case of on-premises deployment managed by Customer, service resilience falls under Customer’s responsibility.

AMS Employee Self Service:

- Data backup: Azure Cosmos DB default backup policy is being used:
    - All the backups are stored separately in a storage service, and those backups are globally replicated for resiliency against regional disasters.
    - Data is backed up every 4 hours, the last 8 hours of backups are kept,
    - SITA shall delete all data backup without further notice to Customer within 10 days following the end of the configured backup data retention period,
    - Backups are automatically deleted as soon as the 8 hours retention period is reached.
- Data backup protection: backups are encrypted in Azure Cosmos DB,
- 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 cloud security measures are implemented for the Service:

AMS Core v6:

SITA ATI Cloud option:

- 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 includes compute, network, storage and management plane redundancies, to ensure 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 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) and Recovery Point Objective (RPO) are documented and agreed upon within agreements with Customers.

Azure hosted option:

- Datacenter access restriction, cloud backup recovery testing: standard Microsoft Azure security measures are implemented, please refer to Microsoft Product and Services DPA protection addendum – Appendix A – Security Measures.
- Cloud infrastructure redundancy: Microsoft Azure cloud is deployed across availability zones.

AMS Employee Self Service:

- Datacenter access restriction: AMS Employee Self Service being hosted in Azure, please refer to Microsoft Product and Services DPA protection addendum – Appendix A – Security measures, available on Microsoft Licensing Resources and Documents webpage.
- Azure Advisor security baseline is used, and recommendations followed and implemented.

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)