SITA SUPPLIER DATA PROCESSING AGREEMENT

DEFINITIONS & INTERPRETATION

The following definitions and interpretation apply in this Data Processing Agreement ("DPA"):

The terms "**personal data**", "**controller**", "**processor**", "**processing**", "**data subject**", shall bear the meaning ascribed under Regulation (EU) 2016/679 (as applicable), and the term "**process**" shall be construed accordingly.

"**Affiliate**" has the meaning ascribed to it in the Agreement and, if not defined in the Agreement, means with respect to any person, any entity that directly or indirectly through one or more intermediaries Controls or is Controlled by such person or is under direct or indirect common Control with such person. "**Control**" means, in respect of an entity, the ability (whether it is legally enforceable or not) to control, whether directly or indirectly, the composition of the board of directors (or other governing body) of that entity, the voting rights of the majority of voting securities of the entity, or the management of the affairs of that entity.

"**Agreement**" means the agreement to which this DPA is incorporated into on the later of the date of execution of the Agreement or 26th May 2018.

"**Data Protection Law**" means the Directive and the Regulations (as amended or replaced from time to time), guidance, directions, determinations, codes of practice, circulars, orders, notices or demands issued by any Supervisory Authority and any applicable national, international, regional, municipal or other data privacy and data protection laws or regulations in any other territory in which the Services are provided or which are otherwise applicable.

"**Directive**" means the the European Privacy and Electronic Communications Directive (Directive 2002/58/EC).

"**Regulations**" means:

1. Regulation (EU) 2016/679 (as amended or replaced from time to time) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; and

2. on and from the date on which it becomes effective, the proposed regulation on Privacy and Electronic Communications concerning the respect for private life and the protection of personal data in electronic communications.

"**Restricted Transfer**" means:

1. a transfer of SITA Personal Data from SITA to SUPPLIER; and

2. an onward transfer of SITA Personal Data from SUPPLIER to SUPPLIER's Sub-processor (including any SUPPLIER Affiliate), or between two establishments of SUPPLIER.

in each case, where such transfer would be prohibited by Data Protection Law (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Law) in the absence of the Standard Contractual Clauses to be established under clause 1.4 or clause 1.5(c)(iii) below.

"**Services**" means the services and any products provided by SUPPLIER to SITA pursuant to the Agreement.

"**SITA**" means the relevant subsidiary within the SITA group of companies which is a party to the Agreement to which this DPA is incorporated, and its Affiliates receiving Services from SUPPLIER.

"**SITA Data**" means all data (including non-personal data and SITA Personal Data) in whatever form or medium which is (i) supplied, or in respect of which access is granted to SUPPLIER (or any approved third party) whether by SITA or otherwise in connection with the Agreement, or (ii) produced or generated by or on behalf of SUPPLIER (or any approved third party) in connection with the Agreement.

"**SITA Personal Data**" means all personal data in whatever form or medium which is (i) supplied, or in respect of which access is granted to SUPPLIER (or any approved third party) whether by SITA or otherwise in connection with the Agreement, or (ii) produced or generated by or on behalf of SUPPLIER (or any approved third party) in connection with the Agreement.

"**Standard Contractual Clauses**" means the standard EU contractual clauses described in Part B of this DPA.

"**Sub-processor"** means a processor other than SITA engaged by SITA to process SITA Data in connection with the Services (such as SUPPLIER), or engaged by SUPPLIER to process SITA Data in connection with the Services (such as third parties or SUPPLIER Affiliates).

"**Supervisory Authority**" means any competent data protection or privacy authority in any jurisdiction in which SITA is established, SUPPLIER provides the Services and/or in which SUPPLIER processes personal data.

"**SUPPLIER**" means the party providing the Services to SITA under the Agreement to which this DPA is attached, and any of its Affiliates.

Terms and expressions used in this DPA and not defined herein have the meanings assigned to them in the Agreement to which this DPA is attached.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT, IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THE TERMS OF THE AGREEMENT (OTHER THAN THIS DPA) AND THE TERMS OF THIS DPA, THE TERMS OF THIS DPA WILL PREVAIL.

PART A – DATA PROTECTION

1. Data Protection

1.1 SUPPLIER and SITA hereby agree that for the purposes of this DPA and SUPPLIER's processing of the SITA Personal Data in connection with the Services to be provided, SUPPLIER (and each permitted Sub-processor pursuant to this DPA) shall be a processor and/or Sub-processor.

1.2 The Parties agree the following sets out the information required by Regulation (EU) 2016/679:

Subject matter of processing	The provision of the Services
Duration of processing	Duration of the Agreement

Nature of processing	SUPPLIER processes SITA Personal Data in connection with the provision of the Services.
Purpose of processing	To provide the Services
Type of personal data	Includes any of the following accessed by, provided to, or processed by SUPPLIER during the provision of the Services: **[*DRAFTING NOTE: Delete bullet(s) if not applicable to the processing under the agreement]*** • Names, contact details, and passenger, travel, and baggage data of passengers/customers of SITA's customers. • Names, and contact details, and other personal data of employees and contractors of SITA's customers and suppliers. • Names, and contact details, and other personal data of SITA's employees and contractors.
Categories of data subjects	**[*DRAFTING NOTE: Delete bullet(s) if not applicable to the processing under the agreement]*** • Passengers/customers of SITA's customers. • Employees/contractors of SITA's customers and suppliers • Employees/contractors of SITA.

1.3 SUPPLIER, acting as processor and/or Sub-processor, will:

(a) only process the SITA Personal Data in compliance with, and shall not cause itself or SITA to be in breach of, Data Protection Law;

(b) only process the SITA Personal Data on the documented instructions of SITA as specified in the Agreement and otherwise as necessary to perform its obligations under this Agreement;

(c) notify SITA in case SUPPLIER is of the opinion that an instruction of SITA is not in compliance with Data Protection Law.

(d) take all reasonable steps to ensure any staff who may have access to SITA Data are subject to appropriate obligations of confidentiality and at all times act in compliance with Data Protection Law and the obligations of this Clause 1;

(e) implement all appropriate technical and organisational measures to ensure security of the SITA Personal Data including protection against unauthorised or unlawful processing (including without limitation unauthorised or unlawful disclosure of, access to and/or alteration of SITA Data) and against accidental loss, destruction or damage. SUPPLIER confirms such measures shall:

(i) ensure a level of security appropriate to the risks presented by the processing of SITA Personal Data;

(ii) comply with Data Protection Law at all times; and

(iii) comply with security requirements as described in Part C, as reasonably updated and notified from time to time;

(f) implement appropriate technical and organisational measures to provide SITA with co-operation and assistance in performing data protection impact assessments and complying with any data subject rights (including access requests) received by, or on behalf of, SITA;

(g) subject to, and save where authorized to transfer to its Sub-processors as set forth in clause 1.5, not transfer and/or disclose any SITA Personal Data to any other party without the prior specific written consent of SITA and unless permitted by Data Protection Law;

(h) save where SUPPLIER has in respect of a particular Sub-processor complied with the requirement to enter into the Standard Contractual Clauses with the Sub-processor as set forth in clause 1.5(c)(iii) and with clauses 1.5(c)(i) and (ii), not transfer any SITA Personal Data outside the European Economic Area (**EEA**) or to any international organisations without the express prior written consent of SITA;

(i) permit SITA, or a third-party auditor acting under SITA's direction, to conduct, at SITA's cost, data privacy and security audits, assessments and inspections concerning SUPPLIER's data security and privacy procedures relating to the processing of SITA Personal Data, its compliance with this Clause 1 and Data Protection Law. SITA may, in its sole discretion, require SUPPLIER to provide evidence of SUPPLIER's compliance with this DPA and these procedures in lieu of conducting such an audit, assessment or inspection;

(j) notify SITA in writing without undue delay, but at least within 48 hours after it becomes aware of any unauthorised or unlawful processing, disclosure of, or access to, SITA Data and/or any accidental or unlawful destruction of, loss of, alteration to, or corruption of SITA Data (a **Data Breach**) and provide SITA, as soon as possible, with complete information relating to a Data Breach, including, without limitation, the nature of the Data Breach and estimated duration of the breach , the nature of the personal data affected, the categories and number of data subjects concerned, the number of personal data records concerned, measures taken or proposed by SUPPLIER to address the Data Breach and the possible adverse effect of the Data Breach, the name and contact details of relevant internal and external stakeholders where more information can be obtained. SUPPLIER shall maintain a log of Data Breaches including facts, effects, investigative steps, conclusions and remedial action taken. Where it is possible to do so, SUPPLIER shall take all steps to restore, re-constitute and/or reconstruct any SITA Data which is lost, damaged, destroyed, altered or corrupted as a result of a Data Breach as if they were SUPPLIER's own data at its own cost with all possible speed and shall provide SITA with all reasonable assistance in respect of any such Data Breach. Without the prior written authorisation of SITA, SUPPLIER will not notify and/or disclose any information relating to a Data Breach to any third party, including but not limited to data subjects and supervisory authorities, unless required by law to do so (in which case, and if not prohibited by law, SUPPLIER will provide reasonable notice to SITA of such a requirement);

(k) on termination or expiry of the Agreement, for whatever reason, cease all use of the SITA Data and shall, at SITA's election, either destroy all SITA Data or transfer all SITA Data to SITA or a nominated third party (in a mutually agreed format and by a mutually agreed method); and

(l) inform SITA immediately of any enquiry, complaint, notice or other communication it receives from any Supervisory Authority or any individual, relating to either SUPPLIER's or third parties' appointed by SUPPLIER in connection with the Services or SITA's compliance with Data Protection Law. SUPPLIER shall provide all necessary assistance to SITA to enable SITA to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Law. For the avoidance of doubt, SUPPLIER shall not respond to any such enquiry, complaint, notice or other communication without the prior written consent of SITA.

1.4 **Restricted Transfers.** SITA (as "data exporter") and SUPPLIER (as “data importer”) hereby enter into either the:

(1) Standard Contractual Clauses (Module 2: Controller to Processor) where SITA is a controller; or (2) Standard Contractual Clauses (Module 3: Processor to Processor) where SITA is a processor; and addendum in the case of transfers out of the UK

in the manner described in Part B in respect of any Restricted Transfers:

(a) from SITA to SUPPLIER; and/or

(b) where both SITA and SUPPLIER are outside of both the EEA and a third country subject to an adequacy decision under the GDPR, and SUPPLIER processes personal data, received by onward transfer from SITA, originating from any data subjects specified in clause 1.2 that are EEA-resident (e.g. EEA-resident passengers, customers, employees and contractors).

1.5 **Sub-processors**. SITA authorises SUPPLIER to appoint or sub-contract Sub-processors in accordance with this section 1.5 and any restrictions in this Agreement:

(a) SUPPLIER may continue to use those Sub-processors already engaged by SUPPLIER as at the date of entry into this DPA, subject to SUPPLIER in each case as soon as practicable meeting the obligations set out in clause 1.5(c).

(b) SUPPLIER shall give SITA prior written notice of the appointment of any new Sub-processor, including full details of the processing to be undertaken by the Sub-processor. If within 30 days of receipt of that notice, SITA notifies SUPPLIER in writing of any objections (on reasonable grounds) to the proposed appointment:

(i) SUPPLIER shall work with SITA in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor (including but not limited to appointing an alternative Sub-processor satisfactory to SITA); and

(ii) Where such a change cannot be made within 60 days from SUPPLIER's receipt of SITA's notice, notwithstanding anything in the Agreement, SITA may by written notice to SUPPLIER with immediate effect terminate the Services which require the use of the proposed Sub-processor, with no further liability to SITA other than to pay fees for the Services up to date of termination (and SITA shall be refunded for any advance payment of fees for Services following the date of termination).

(c) With respect to each Sub-processor, SUPPLIER shall:

(i) Before the Sub-processor first processes SITA Data (or, where relevant, in accordance with clause 1.5(a)), carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for SITA Data required by this Agreement;

(ii) enter into a written agreement with all Sub-processors containing obligations on such Sub-processors which are no less onerous than those set out in this DPA.

(iii) enter into: Standard Contractual Clauses (and addendum in the case of transfers out of the UK)with all Sub-processors: (1) where there is any Restricted Transfer between SUPPLIER and the Sub-processor; and/or (2) where SUPPLIER and its Sub-processor are both outside of both the EEA and a third country subject to an adequacy decision under the GDPR, and Sub-Processor processes personal data, received by onward transfer from SUPPLIER, originating from any data subjects specified in clause 1.2 that are EEA-resident (e.g. EEA-resident passengers, customers, employees or contractors); and

(iv) provide to SITA for review such copies of its above agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Annexure) as SITA may request from time to time.

1.6 SUPPLIER will provide SITA with such assistance and co-operation as SITA may reasonably request to enable SITA to comply with any of its obligations under Data Protection Law, including but not limited to obligations in connection with data subject rights and data processing impact assessments.

1.7 SUPPLIER shall, immediately on demand, fully indemnify SITA and keep SITA fully and effectively indemnified against all costs, claims, demands, expenses (including legal costs and disbursements on a full indemnity basis), losses (including indirect losses and loss of profits), actions, proceedings and liabilities of whatsoever nature arising from or incurred by SITA in connection with any failure of SUPPLIER or any third party appointed by SUPPLIER to comply with the provisions of this Clause 1, and Standard Contractual Clauses entered into between the parties, and/or Data Protection Law in respect of its processing of SITA Data. The parties agree that the indemnity in this clause is not limited by any monetary cap on liability contained in the Agreement.

1.8 SUPPLIER is obligated to provide all reasonable assistance to SITA, including but not limited to any reasonable requests to amend this Agreement, or the Standard Contractual Clauses (and addendum in the case of transfers out of the UK) between the parties, based on changes in Data Protection Law.

PART B – STANDARD CONTRACTUAL CLAUSES & THIRD COUNTRY PROCESSING AGREEMENTS

1. Standard Contractual Clauses

1.1 Standard data protection clauses adopted by the European Commission pursuant to Article 46(2) of Regulation (EU) 2016/679 (and for transfers out of the UK, the addition of an addendum to such standard contractual clauses, as approved by the UK Information Commissioners Office) for the transfer of personal data to data importers established in third countries which have not received an adequacy decision pursuant to Article 45(3) of Regulation (EU) 2106/679, are available at the following web addresses:

(a) For Module 2 (Controller to Processor) transfers: https://www.sita.aero/gdpr/scc/suppliers/module2

(b) For Module 3 (Processor to Processor) transfers: https://www.sita.aero/gdpr/scc/suppliers/module3

("**the Standard Contractual Clauses**") and

(c) the addendum for transfers out of the UK: https://www.sita.aero/gdpr/scc/UKaddendum.

1.2 The parties agree that: (1) that the Standard Contractual Clauses (and for transfers out of the UK, the addition of an addendum to such standard contractual clauses, as approved by the UK Information Commissioners Office) referred to above are incorporated into and form an integral part of this DPA and the Agreement, as if they were set out in full in this Part B; and (2) that by executing this DPA the parties indicate their acceptance of the aforesaid incorporation of said Standard Contractual Clauses.

1.3 The parties agree that they enter into the Standard Contractual Clauses pursuant to clause 1.4 of Part A, and the party, processing, execution, and security measure details of such Standard Contractual Clauses are as follows:

(a) **Name of the data exporting entity**: The SITA entity recorded in the Agreement and any of its Affiliates exporting data from the EEA to the data importer.

(b) **Data exporter address**: the address of the SITA entity recorded in the Agreement.

(c) **Name of the data importing entity**: The SUPPLIER entity recorded in the Agreement and any of its Affiliates importing data from the data importer.

(d) **Data importer address**: the address of the SITA entity recorded in the Agreement.

(e) **Governing law and choice of forum and jurisdiction for Standard Contractual Clauses 17 and 18**: in each case of data exporting, the law of the Member State from which SITA or its Affiliate is exporting data.

(f) **Execution of the Standard Contractual Clauses** (including in Appendix 1 of the clauses): by entering into this DPA the parties indicate their signing and execution of the Standard Contractual Clauses (including on behalf of their Affiliates providing or receiving the Service).

(g) **In Annex I of the Standard Contractual Clauses**:

(i) **The data exporter**: SITA exports the categories of personal data of the data subjects listed in clause 1.2 of Part A.

(ii) **The data importer**: SUPPLIER imports the categories of personal data of the data subjects listed in clause 1.2 of Part A.

(iii) **The data subjects and categories of personal data**: as listed in clause 1.2 of Part A.

(iv) **Special categories of data**: none, except the following where transferred to or processed by SUPPLIER in connection with the Services: any meal preferences, disability information, or biometric data of any airline passengers, and any health data for HR/sick leave/ employment purposes of SITA employees or contractors. Where such special category data is processed in connection with the Services, restrictions and safeguards detailed within the Agreement will be applied.

(v) **Frequency of the transfer:** on a continuous/regular basis for the duration of the Agreement.

(vi) **Nature of the processing**: the Services provided by the data importer.

(vii) **Purpose of the data transfer and further processing:** in connection with the Services under the Agreement.

(viii) **Period of data retention:** in accordance with the Agreement, and for no longer than the duration of the Agreement.

(ix) **Competent Supervisory Authority:** The Belgian Data Protection Authority.

(h) **In Appendix 2 of the Standard Contractual Clauses, description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 8.6 and 10**: As specified in Part C of this DPA.

1.4 The parties agree the Standard Contractual Clauses to be entered into by SUPPLIER and its Sub-processors pursuant to clause 1.5(c)(iii) of Part A, must adequately describe the data subjects and categories of SITA Personal Data processed by said Sub-processors on SUPPLIER's behalf.

PART C – SUPPLIER SECURITY

1. General Security Provisions

1.1 SUPPLIER shall comply with either 1.1(a) or 1.1(b) below:

(a) SUPPLIER shall maintain and comply with the following certifications during the term of this Agreement, that cover the Services and their associated systems, networks, applications, and underlying components, and shall at all times during the term of this Agreement maintain and perform the technical and organisational security measures included in such certifications:

ISO/IEC 27001 certification;
ISAE3402 SOC2 Type II report;
PCI DSS compliance (where credit card data is handled);

SUPPLIER shall provide evidence of such certifications and documentation to SITA no less than once per calendar year. The standards specified in this clause shall be replaced by future equivalent standards if/when such standards are superseded.

(b) If SUPPLIER does not maintain and comply with the certifications required by clause 1.1(a) above, SUPPLIER shall during the term of this Agreement comply with the detailed security requirements in clause 2.1 below in respect of the Services and their associated systems, networks, applications, and underlying components.

1.2 SUPPLIER shall plan and maintain disaster recovery and business continuity management programs to counteract interruptions and protect critical business processes from the effects of major failures and disasters. These programs must be tested at least annually and comply with ISO 20000, 27002, and 15408.

1.3 SUPPLIER shall comply with all applicable data privacy legislation in respect of the Services.

1.4 SUPPLIER agrees and warrants to SITA that the Services and/or products and/or deliverables and/or supporting systems (as appropriate) supplied by the SUPPLIER to SITA under this Agreement are appropriate to the risk, using all applicable preventative, detective and corrective measures, administrative, physical and technical controls, to ensure SITA Data and information systems are appropriately protected from unauthorized disclosure, alteration and unavailability

1.5 SUPPLIER shall report to SITA, within 24 hours of discovery, any known or suspected unauthorized access, use, misuse, disclosure, destruction, theft, vandalism, modification, or transfer of SITA proprietary information or data. Reports should be by sent via email to the SITA Security Incident Response Team (SIRT@SITA.aero). SUPPLIER will provide SITA with reasonably requested support and information about such security incident and status of any SUPPLIER remediation and restoration activities.

1.6 SUPPLIER will designate a Security Point of Contact within SUPPLIER's organization to act as the liaison between SITA and SUPPLIER.

1.7 SITA may audit compliance of SUPPLIER with Clauses 1.1 & 1.2 above once per calendar year.

1.8 Without prejudice to SITA's rights to audit SUPPLIER under this Part C, SUPPLIER shall provide to SITA reports and information demonstrating compliance with specific security measures set forth in this Part C, if and when requested by SITA, at no additional charge.

1.9 Except to the extent the liability arises as a result of the action or omission of SITA, SUPPLIER shall indemnify, protect and hold harmless SITA against any liability

whatsoever incurred by SITA, including any reasonable costs, claims, demands and expenses arising out of or in connection with such liability (including reasonable legal costs), arising from any failure to perform, and/or failure to comply with the requirements of this Part C, and/or arising from any breach of Clauses 1.1 or 1.2.

1.10 SUPPLIER will maintain and follow documented incident response policies consistent with industry best practices and will comply with data breach notification terms of the Agreement. SUPPLIER will investigate unauthorized access and unauthorized use of SITA Personal Data of which SUPPLIER becomes aware (security incident), and, within the Service scope, SUPPLIER will define and execute an appropriate response plan.

2. Detailed Security Requirements if Supplier does not comply with the Certifications required by clause 1.1(a).

2.1. If SUPPLIER does not maintain and comply with the certifications required in clause 1.1(a), it must instead maintain and comply with all the following requirements:

a) SUPPLIER will maintain and follow IT security policies and practices that are integral to SUPPLIER's business and mandatory for all SUPPLIER employees, including supplemental personnel.

b) SUPPLIER will review its IT security policies at least annually and amend such policies as SUPPLIER deems reasonable. SUPPLIER will notify SITA of any changes to the Provider's security policy.

c) SUPPLIER will maintain and follow its standard mandatory employment verification requirements for all new hires, including supplemental employees, and extend such requirements to wholly owned SUPPLIER subsidiaries. These requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by SUPPLIER.

d) SUPPLIER employees will undergo security and privacy training and awareness to ensure they comply with SUPPLIER 's security policies, and records of training should be maintained.

e) SUPPLIER will ensure that all employees and representatives who will perform work or have access to information resources associated with SITA are covered by binding/signed non-disclosure agreements

f) SUPPLIER will ensure that physical SUPPLIER related work areas are secure to prevent unauthorized physical access, damage and interference. SUPPLIER will restrict and limit access to SITA Data and SITA information systems by defining roles and segregating duties (to avoid conflicts of interest in security activities), establishing authorization processes and by implementing a technical solution that manages the access rights of users from their onboarding to the end of their assignment and access rights. Access rights to SITA Data and information systems will be periodically reviewed

g) Consistent with industry standard practices, and to the extent supported by each component managed by SUPPLIER within the Service, SUPPLIER will enforce timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, implement dual-factor authentication whenever possible, ensure accesses are uniquely identifying a person and/or a system and maintain sufficient audit records of accesses for at least thirty days. SUPPLIER will ensure that authentication mechanisms cannot be overcome.

h) SUPPLIER will limit the number of privileged users and will appropriately monitor their access with extensive logging.

i) SUPPLIER personnel remotely accessing Systems and data in relation to the Service will be individually identified and authenticated using two-factor authentication, and their login attempts will be monitored.

j) SUPPLIER will ensure that the termination process for its employees includes return of, and revoking of access rights to, all SITA information assets.

k) SUPPLIER shall maintain logs of all Events on systems and networks used to process Personal Data ("Event Logs"), including information such as date, time, user ID, device

accessed, and port used. SUPPLIER shall maintain such Event Logs for a minimum period of twelve (12) months. If requested by SITA, SUPPLIER shall allow SITA to analyze the Event Logs for security related events, unusual activities and other issues, such as unsuccessful attempts to create backup copies of data. For the purpose of this section, "**Event**" shall mean: any incident that may result in damage to any information security assets, Personal Data, and/or operations of systems and networks.

l) SUPPLIER will secure all SITA Data by encrypting the data and/or the link between the two communication ends, using reliable implementations of network protocols and encryption algorithms, in compliance with legal requirements in the country of operation and as recommended by security best practices. SUPPLIER will communicate to SITA the secure network protocols and encryption algorithms used.

m) SUPPLIER will encrypt SITA stored sensitive data, including personal data, on all information systems deemed sensitive, using reliable encryption algorithms (compliant with FIPS 140-2) in compliance with legal requirements in the country of operation and as recommended by security best practices.

n) SUPPLIER will perform or have performed annual penetration testing on all deemed sensitive information systems or upon major service changes, while avoiding operational and business disruption.

o) SUPPLIER will implement antimalware solution on all relevant information systems.

p) SUPPLIER will subscribe to an external threat intelligence service in order to receive regular timely information of current threats and technical vulnerabilities for all relevant information systems. SUPPLIER will build a patch management process based on current best practice

q) SUPPLIER will implement Next Generation firewalls with dedicated rulesets/policies that will be periodically reviewed as part as the general security review process. The technologies used will be regularly updated as part of the patch and vulnerability management process.

r) SUPPLIER will perform automatic vulnerability scanning, while avoiding operational and business disruption.

s) SUPPLIER will assess business impacts and security risks regarding all relevant information systems, at least annually and upon any major change in the operating environment.

t) SUPPLIER will implement an effective backup and restore strategy regarding SITA Data, and implement reliable technology to support its strategy. Backed up data at rest should be encrypted within its container, data sent between the backup server and the backed-up resources should be encrypted in transit. At least one backup copy should be kept on a remote location, not subject to natural threats (e.g. flood).