SECOND AMENDMENT
TO CONTRACT DA-5446
BETWEEN
THE CITY OF LOS ANGELES
AND
SITA INFORMATION NETWORKING COMPUTING USA, INC.
TO
PROVIDE PROFESSIONAL SERVICES
FOR THE DEPARTMENT OF AIRPORTS
FOR THE CITY OF LOS ANGELES

THIS SECOND AMENDMENT to Agreement DA-5446 between The City of Los Angeles and Sita Information Networking Computing USA, Inc. is entered into this ___ day of _____, 202_ at Los Angeles, California, by and between the **CITY OF LOS ANGELES,** acting by and through its Board of Airport Commissioners ("Board") of its Department of Airports ("Los Angeles World Airports" or "LAWA"), and Sita Information Networking Computing USA, Inc. ("SITA").

RECITALS

WHEREAS on May 24, 2020, LAWA entered into this Agreement (DA-5446) with SITA to implement, operate and maintain a Consolidated Common Use Platform at Los Angeles International Airport (the "CCUP System Agreement").

WHEREAS on June 26, 2024**,** the parties entered into the First Amendment to this Agreement (DL-5546A) adding a new Section 33 which states:

> 33.0 As of April 1, 2022, SITA shall perform the CCUP Services for the Common Use Airlines in the Bradley International Terminal and Terminal S pursuant to this Agreement.
>
> > 33.1 As of April 1, 2022, the cost of the Terminal Space SITA occupies to support CCUP Services for the Common Use Carriers in the Bradley Terminal and Terminal S under this Agreement will be absorbed by LAWA.

WHEREAS the parties now wish to increase the Agreement authority by Seven Million Dollars ($7,000,000) for a total of Thirty-Six Million One Hundred Seven Thousand Three Hundred Seventy-Nine Dollars ($36,107,379);

WHEREAS the parties now also wish to add required Mandatory Federal Terms and clarify LAWA Information Security Requirements;

NOW, THEREFORE, for and in consideration of the covenants and conditions hereinafter contained to be kept and performed by the respective parties hereto, IT IS **MUTUALLY AGREED** as follows:

AMENDMENT

Section 1. Section 3.2 of the Agreement is amended as follows:

The phrase "Twenty-Nine Million One Hundred Seven Thousand Three Hundred Seventy-Nine Dollars ($29,107,379)" is deleted and replaced with the phrase "Thirty-Six Million One Hundred Seven Thousand Three Hundred Seventy-Nine Dollars ($36,107,379)."

Section 2. Section 18.0 of the Agreement is amended to add a new Section 18.5 (and Attachment One) including the Mandatory Federal Terms set forth below:

"18.5 Civil Rights – General; Civil Rights – Title VI Assurances - 49 CFR § 21.7(a)(1); 49 CFR Part 21 Appendix C (b); and as amended or interpreted from time to time.

18.5.1 Civil Rights – General – 49 USC § 47123, derived from the Airport and Airway Improvement Act of 1982, Section 520. In all its activities within the scope of its airport program, the Contractor agrees to comply with pertinent statutes, Executive Orders, and such rules as identified in Title VI List of Pertinent Nondiscrimination Acts and Authorities to ensure that no person shall, on the grounds of race, color, national origin (including limited English proficiency), creed, sex (including sexual orientation and gender identity), age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

This provision is in addition to that required by Title VI of the Civil Rights Act of 1964.

The above provision binds the Contractor and subcontractors from the bid solicitation period through the completion of the contract. If the Contractor transfers its obligation to another, the transferee is obligated in the same manner as the Contractor. The above provision obligates the Contractor for the period during which the property is owned, used or possessed by the Contractor and the airport remains obligated to the Federal Aviation Administration.

18.5.2 Civil Rights – Title VI Assurances – 49 USC § 47123, FAA Order 1400.11, and U.S. Department of Transportation Order DOT 1050.2, Standard Title VI Assurances and Nondiscrimination Provisions, effective April 24, 2013. Contractor further agrees to comply with all applicable US DOT Standard Title VI/Non-Discrimination, set forth in Attachment One (Civil Rights – Title VI Assurances) and made a material term of this Contract, as such requirements may

be amended or interpreted by the FAA or the United States Department of Transportation from time to time; specifically, the following clauses as provided in Attachment One:

a. Title VI List of Pertinent Nondiscrimination Acts and Authorities
b. Compliance with Nondiscrimination Requirements

18.5.3 Audit of Subcontracts. LAWA may conduct a review of the Contractor's compliance with this Section 18.5. Contractor must cooperate with LAWA throughout the review process by supplying all requested information and documentation to LAWA, making Contractor staff and officials available for meetings as requested, and correcting any areas of non-compliance as determined by LAWA.

18.5.4 Contractor agrees that it shall insert the provisions found in Sections 18.5.1 and 18.5.2, inclusive of Attachment One, in any solicitation, subcontract, sublease, assignment, license, transfer, or permit, or other instrument, by which said Contractor grants a right or privilege to any person, firm, or corporation under this Contract."

"Attachment One" (Civil Rights – Title VI Assurances) is attached to this Second Amendment and incorporated by reference herein.

Section 3. Section 19.1(b) of the Agreement is amended to add the following text and the Attachment Two referenced therein:

"Without limiting the generality of this Section 19(b) and Section 18.0 (Restrictions and Regulations), Contractor shall develop, implement and maintain during the term of this Contract pursuant to Section 1.0 (Term of Contract) the information security requirements contained in Attachment Two (LAWA Information Security Requirements) and incorporated by reference herein. The Contractor acknowledges and agrees that Attachment Two shall be updated from time-to-time by LAWA, in its sole discretion after consultation with Contractor, to be effective thirty (30) days following notice to Contractor pursuant to Section 7.2 (Notice to Contractor). Once effective, each such update to Attachment Two shall be integrated into the Agreement as Attachment Two replacing the existing Attachment Two entirely. For the avoidance of doubt, any amendment to Attachment Two (LAWA Information Security Requirements) shall be made after the Parties come to the table to discuss the requested amendment."

"All cyber security measures Contractor is required to perform which are listed in or described as available (ability to) in Attachment Two will not require additional compensation. Cyber security measures requested by LAWA required of Contractor not listed in or described as available (ability to) in Attachment Two hereof may, if a Material Addition or Change, be subject to Section 3.9"

"Attachment Two" (LAWA Information Security Requirements) is attached to this Second Amendment and incorporated by reference herein."

Section 4. Section 3.1 of the agreement is amended to insert the following at the end of Section 3.1:

"Contractor further agrees to provide the Services to City under the contractual terms and conditions set forth in Attachments 1 and 2 which are attached hereto and incorporated by reference herein."

Section 5. Except as amended or modified by this Second Amendment, the Agreement is hereby ratified and confirmed and all other terms of the Agreement shall remain in full force and effect, unaltered and unchanged by this Second Amendment. If there is any conflict between the provisions of this Second Amendment and the provisions of the Agreement, the provisions of this Second Amendment shall prevail. Whether or not specifically amended by this Second Amendment, all terms and provisions of the Agreement are amended to the extent necessary to give effect to the purpose and intent of this Second Amendment.

Section 6. No provisions of the Agreement or this Second Amendment may be amended or added to except by a written agreement signed by the Parties or their respective successors-in-interest. This Second Amendment is not intended to confer upon any person other than the Parties, any rights or remedies hereunder.

Section 7. This Second Amendment shall be governed by, and construed in accordance with, the laws of the State of California. The Agreement and this Second Amendment are subject to the provisions of the Los Angeles Administrative Code. Each Party represents and warrants that this Second Amendment has been negotiated and drafted at arms-length by equally sophisticated parties, and any ambiguity cannot be attributed to either Party hereto. If any provision of this Second Amendment, or the application thereof to any persons or circumstances, shall be invalid or unenforceable, the remainder of this Second Amendment shall not be affected thereby, and each provision of this Second Amendment shall be valid and shall be enforceable to the fullest extent permitted by law.

Section 8. This Second Amendment and any other document necessary for the consummation of the transaction contemplated by this Second Amendment may be executed in counterparts, including counterparts that are manually executed and counterparts that are in the form of electronic records and are electronically executed. An electronic signature means a signature that is executed by symbol attached to or logically associated with a record and adopted by a party with the intent to sign such record, including facsimile or e-mail signatures. All executed counterparts shall constitute one agreement, and each counterpart shall be deemed an original. The parties hereby acknowledge and agree that electronic records and electronic signatures, as well as facsimile signatures, may be used in connection with the execution of this Second Amendment and electronic signatures, facsimile signatures or signatures transmitted by electronic mail in so-called PDF format shall be legal and binding and shall have the same full force and effect as if a paper original of this Second Amendment had been delivered that had been signed using a handwritten signature. All parties to this Second Amendment

(i) agree that an electronic signature, whether digital or encrypted, of a party to this Second Amendment is intended to authenticate this writing and to have the same force and effect as a manual signature; (ii) intended to be bound by the signatures (whether original, faxed, or electronic) on any document sent or delivered by facsimile or electronic mail or other electronic means; (iii) are aware that the other party(ies) will rely on such signatures; and, (iv) hereby waive any defenses to the enforcement of the terms of this Second Amendment based on the foregoing forms of signature. If this Second Amendment has been executed by electronic signature, all parties executing this document are expressly consenting, under the United States Federal Electronic Signatures in Global and National Commerce Act of 2000 ("E-SIGN") and the California Uniform Electronic Transactions Act ("UETA") (California· Civil Code §1633.1 et seq.), that a signature by fax, e-mail, or other electronic means shall constitute an Electronic Signature to an Electronic Record under both E-SIGN and UETA with respect to this specific transaction.

REMAINDER OF THIS PAGE IS BLANK

IN WITNESS WHEREOF, City has caused this Contract to be executed by the CEO of its Department of Airports, and Contractor has caused the same to be executed by its duly authorized officers, all as of the day and year first hereinabove written.

APPROVED AS TO FORM:
Hydee Feldstein Soto, City Attorney

Date: _____

By: _____
Deputy City Attorney

CITY OF LOS ANGELES
By signing below, the signatory attests that they have no personal, financial, beneficial, or familial interest in this Contract.

By: _____
Chief Executive Officer
Department of Airports

SITA INFORMATION NETWORKING COMPUTING USA, INC.

By: Signed by: Shawn Gregor 5A769AEDA6C84B0... (Signature)

Shawn Gregor
Print Name

President
Print Title

SITA INFORMATION NETWORKING COMPUTING USA, INC.

By: Signed by: Catharine Young BC63F108AD9E4F8... Signature

Catharine C. Young
Print Name

Assistant Secretary
Print Title

APPROVED AS TO FORM:

Date: _____

By: _____

ATTACHMENT ONE

Mandatory Federal Terms

ATTACHMENT ONE

CIVIL RIGHTS – TITLE VI ASSURANCES

Civil Rights – Title VI Assurances. In accordance with, and as amended or interpreted from time to time, 49 USC § 47123, FAA Order 1400.11, and U.S. Department of Transportation Order DOT 1050.2, Standard Title VI Assurances and Nondiscrimination Provisions, effective April 24, 2013.

I. Title VI List of Pertinent Nondiscrimination Acts and Authorities. During the performance of this contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor") agrees to comply with the following non-discrimination statutes and authorities; including but not limited to:

Title VI of the Civil Rights Act of 1964 (42 USC § 2000d *et seq.*, 78 stat. 252) (prohibits discrimination on the basis of race, color, national origin);

49 CFR part 21 (Non-discrimination in Federally-Assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964);

The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 USC § 4601) (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);

Section 504 of the Rehabilitation Act of 1973 (29 USC § 794 *et seq.*), as amended (prohibits discrimination on the basis of disability); and 49 CFR part 27 (Nondiscrimination on the Basis of Disability in Programs or Activities Receiving Federal Financial Assistance);

The Age Discrimination Act of 1975, as amended (42 USC § 6101 *et seq.*) (prohibits discrimination on the basis of age);

Airport and Airway Improvement Act of 1982 (49 USC § 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);

The Civil Rights Restoration Act of 1987 (PL 100-259) (broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);

Titles II and III of the Americans with Disabilities Act of 1990 (42 USC § 12101, et seq) (prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities) as implemented by U.S. Department of Transportation regulations at 49 CFR parts 37 and 38;

The Federal Aviation Administration's Nondiscrimination statute (49 USC § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);

Executive Order 12898, Federal Actions to Address Environmental Justice in Minority

Populations and Low-Income Populations (ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations);

Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs [70 Fed. Reg. 74087 (2005)];

Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 USC § 1681, et seq).

II. Compliance with Nondiscrimination Requirements. During the performance of this contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor"), agrees as follows:

Compliance with Regulations: The Contractor (hereinafter includes consultants) will comply with the Title VI List of Pertinent Nondiscrimination Acts and Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.

Nondiscrimination: The Contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, national origin (including limited English proficiency), creed, sex (including sexual orientation and gender identity), age, or disability in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The Contractor will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21.

Solicitations for Subcontracts, including Procurements of Materials and Equipment: In all solicitations, either by competitive bidding or negotiation made by the Contractor for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by the Contractor of the contractor's obligations under this contract and the Nondiscrimination Acts and Authorities on the grounds of race, color, or national origin.

Information and Reports: The Contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by LAWA or the Federal Aviation Administration to be pertinent to ascertain compliance with such Nondiscrimination

Acts and Authorities and instructions. Where any information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, the Contractor will so certify to LAWA or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

Sanctions for Noncompliance: In the event of a Contractor's noncompliance with the non-discrimination provisions of this contract, LAWA will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

a. Withholding payments to the Contractor under the contract until the Contractor complies; and/or

b. Cancelling, terminating, or suspending a contract, in whole or in part.

Incorporation of Provisions: The Contractor will include the provisions of paragraphs one through six in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The Contractor will take action with respect to any subcontract or procurement as LAWA or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the Contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the Contractor may request LAWA to enter into any litigation to protect the interests of LAWA. In addition, the Contractor may request the United States to enter into the litigation to protect the interests of the United States.

ATTACHMENT TWO

LAWA Information Security Requirements

Attachment Two

LAWA Information Security Requirements

Contents

This document establishes the minimum information security requirements that Providers must meet when delivering solutions or services to Los Angeles World Airports (LAWA). It defines mandatory controls, design and documentation expectations, assessment and remediation practices, and supplemental requirements for cloud and vendor-hosted systems. Together, these sections ensure LAWA's information, systems, and operations are protected in alignment with industry standards, legal and regulatory obligations, and LAWA's risk tolerance.

LAWA Information Security Requirements

The term 'Information Systems Security' referenced in this section refers to an application or operating systems software and hardware used to host any component of the proposed solution. Internet access provided by Selected Contractor (Provider) can terminate at LAWA network perimeter. LAWA will provide transit connection between the Internet Service Provider (ISP) to internally managed systems. The Provider shall incorporate security best practices and meet a standard of due care to support the security policy of Los Angeles World Airports and shall abide by the following requirements:

A. Security Controls

Providers shall be responsible for configuring security controls to provide individual accountability, audit ability, and separation of duties. Security controls must be consistent with industry best practices, including but not limited to the following:

- Authentication requirements for access to sensitive data and privileged functions.
- Ensure the latest operating system patches have been applied to all components.
- Ensure the latest security-related patches have been applied to allcomponents.
- Run only services required to meet desired functionality (disable unused services).
- Identify and enable required TCP/UDP ports and disable other TCP/UDP ports when applicable.
- Log all security related events including unauthorized attempts to access privileged services.
- For data encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of alength that yields equivalent strength.

B. Security Design & Review

- Provider shall submit a network diagram for approval by LAWA IT Security.
- Provider shall submit an application flow diagram for approval by LAWA ITSecurity.
- Provider shall be required to show that the network and/or application flow design conforms to security best practices.

C. Documentation

Providers shall provide a security plan that includes, but is not limited to:

- An overview of the information system security posture.
- Technical details regarding information system implementation strategy, documentation or guidelines that vendor follows to implement and deliver the information system.
- Technical details regarding security strategy - patches applied, operating system hardening steps, services enabled/disabled, TCP/UDP ports opened/closed, authentication requirements, etc.

- Any deviations from the security best practices shall be documented by the Selected Contractor and must be approved by LAWA IT Security.

D. Security Assessment

Provider shall conduct a security risk assessment (ISO/IEC 27001 and 27005) prior to deployment to ensure appropriate security controls have been designed and implemented. LAWA IT Security, or a third party representing LAWA, shall conduct a security risk assessment prior to final user acceptance, and semi-annually.

E. Security Issue(s) Remediation

Provision for remediation of security issues as requested by LAWA:

- The Provider must immediately remediate vulnerabilities and high-priority security issues identified during a security review or assessment.
- The Provider shall be responsible to remediate high and medium risk level issues within a reasonable timeframe. If the remediation affects the functionality of the system, LAWA IT Security may grant an exception depending on the risk level or use other external security methods to mitigate the risk. Additional security assessments may be performed after remediation for verification purposes at the discretion of LAWA IT Security.
- The Provider shall deliver and maintain secure solutions and services to LAWA and shall ensure such solutions and services remain secure against new and evolving threats. The Provider assumes full responsibility to remediate any vulnerabilities and security issues within the Provider's solutions, services, and systems (including those of its subcontractors and third-party vendors).

F. Cloud Security – Software as a Service (SaaS)

Software-as-a-Service (SaaS) provides LAWA client the capability to use the provider's applications running on a cloud infrastructure. LAWA does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage except for limited user-specific application configuration settings.

Requirements for Provider:

Regulations, Compliance and Audit

- Ability to provide regulations and compliance control solutions.
- Must be SSAE 16 SOC1/SOC2 or ISO 27001/27002 compliant on all hosting facilities and provide LAWA Information Management Technology (IMT) with compliance audit reports semi-annually.

Identity Access Management

- Multi-factor authentication (MFA): Require strong, multi-factor authentication, especially those with privileged access to the cloud environment.
- Least privilege access: Mandate the use of role-based access control (RBAC) to ensure that users and processes are granted only the permissions essential to perform their required tasks.

- Segregation of duties: Require the provider to enforce segregation of duties within its own staff and infrastructure to prevent any single individual from having excessive access or control.

- Ability to provide identity management solutions such as active directory integration and single sign-on for applicable applications and systems.

Data Access and Protection

- Ability to provide data access control solutions.
- Ability to provide data protection, encryption, and segregation solutions.
- Ability to provide data retrieval/removal solutions when the contract terminates.
- Infrastructure security: Network and Endpoint Protection
- Network segregation: Must enforce network segmentation to isolate LAWA resources from other customers and minimize the risk of lateral movement in the event of a breach.
- Firewalls and DDoS protection: Require the use of advanced firewalls and Distributed Denial of Service (DDoS) protection to guard against network-based attacks such as botnet/malware, SQL injection, cross-site scripting, and denial-of-service attacks for internet-facing systems and applications.
- Vulnerability management: The provider should have a documented and effective program for vulnerability scanning, penetration testing, and timely patching of their systems.
- Endpoint security: Must provide antivirus or Endpoint Detection & Response (EDR) solutions.
- Secure configurations: The provider must continuously monitor for and automatically remediate security misconfigurations, which are a leading cause of data breaches in the cloud.
- Physical security: Provide physical security controls for the data centers, including access controls, surveillance, and environmental protection.
- Key Management: Ability to provide key management solutions.

Business Continuity and Disaster Recovery

- Ability to provide business continuity and disaster recovery solutions, such as alternate sites, backup/recovery procedures, recovery point objectives, and recovery time objectives.

Security Monitoring and Incident Response

- Logging and monitoring: Log all access to data and systems in case of a Cyber Security Incident and upon provider consent; where "Cyber Security Incident" means any confirmed breach of confidentiality, to include integrity or availability, of LAWA systems, LAWA Data, or systems or data operated or processed, by Contractor in the provision of Services to LAWA, which is due to the unauthorized or unlawful access, attack, disclosure, disruption, or denial of access and which has occurred on Provider's, and/or or any third-party systems or infrastructure that Provider uses to provide the Services, provided such third-party is under the control of Provider.

- Incident Response: Ability to provide security incident response according to the provider's cybersecurity incident response plan (CIRP).

- Security Notification: Ability to respond and provide immediate notification to LAWA on all security breaches, system failures, and network outages. Share relevant threat intelligence that can help identify and mitigate potential risks.

- Forensics and legal holds: Provide support for LAWA's need for incident forensics and legal hold requirements.

Live Security Feeds and SLAs

- Ability to provide service level agreements on reliability, availability, performance, customer support, and penalties.

Internet Access and Transit Connections

- Internet access provided by the provider can terminate at LAWA's network perimeter. LAWA will provide transit connections between the Provider's Internet Service Provider (ISP) and internally managed systems.

G. Vendor Hosted Systems Service Provider

Vendor Hosted system services are those services where LAWA does not manage or control daily operations, application or system services, infrastructure, network, servers, operating systems, or storage.

Requirements for Vendor Hosted system services:

Regulations, Compliance and Audit

- Must follow industry best practice security standards when providing Industrial Control Systems.
- Must ensure PCI DSS compliance when dealing with payment cards and PII.
- Ability to provide regulations & compliance control solution.

Identity Access Management

- Multi-factor authentication (MFA): Require strong, multi-factor authentication for, especially those with privileged access to the hosted systems.
- Least privilege access: Mandate the use of role-based access control (RBAC) to ensure that users and processes are granted only the permissions essential to perform their required tasks.
- Segregation of duties: Require the provider to enforce segregation of duties within its own staff and infrastructure to prevent any single individual from having excessive access or control.
- Ability to provide identity management solutions such as active directory integration and single sign-on for applicable applications and systems.

Data Access and Protection

- Ability to provide data access control solutions.
- Ability to provide data protection, encryption, and segregation solutions.
- Ability to provide data retrieval/removal solutions when the contract terminates.
- Infrastructure security: Network and Endpoint Protection
- Network segregation: Must enforce network segmentation to isolate LAWA resources from other customers and minimize the risk of lateral movement in the event of a breach.
- Firewalls and DDoS protection: Require the use of advanced firewalls and Distributed Denial of Service (DDoS) protection to guard against network-based attacks such as botnet/malware, SQL injection, cross-site scripting, and denial-of-service attacks for internet-facing systems and applications.
- Vulnerability management: The provider should have a documented and effective program for vulnerability scanning, penetration testing, and timely patching of their systems.
- Endpoint security: Must provide antivirus or Endpoint Detection & Response (EDR) solutions.
- Secure configurations: The provider must continuously monitor for and automatically remediate security misconfigurations, which are a leading cause of data breaches in the cloud.
- Physical security: Provide physical security controls for the data centers, including access controls, surveillance, and environmental protection.
- Key Management: Ability to provide key management solutions.

Business Continuity and Disaster Recovery

- Ability to provide business continuity and disaster recovery solutions, such as alternate sites, backup/recovery procedures, recovery point objectives, and recovery time objectives.

Security Monitoring and Incident Response

- Logging and monitoring: Log all access to data and systems in case of a Cyber Security Incident and upon provider consent; where "Cyber Security Incident" means any confirmed breach of confidentiality, to include integrity or availability, of LAWA systems, LAWA Data, or systems or data operated or processed, by Contractor in the provision of Services to LAWA, which is due to the unauthorized or unlawful access, attack, disclosure, disruption, or denial of access and which has occurred on Provider's, and/or or any third-party systems or infrastructure that Provider uses to provide the Services, provided such third-party is under the control of Provider. .
- Incident Response: Ability to provide security incident response according to the provider's cybersecurity incident response plan (CIRP).
- Security Notification: Ability to respond and provide immediate notification to LAWA on all security breaches, system failures, and network outages. Share relevant threat intelligence that can help

identify and mitigate potential risks.

- Forensics and legal holds: Provide support for LAWA's need for incident forensics and legal hold requirements.

Live Security Feeds and SLAs

- Ability to provide service level agreements on reliability, availability, performance, customer support, and penalties.

Internet Access and Transit Connections

- Internet access provided by the provider can terminate at LAWA's network perimeter. LAWA will provide transit connections between the provider's Internet Service Provider (ISP) and internally managed systems.

H. Vendor Cybersecurity Standard and Practice

This standard defines the minimum cybersecurity requirements for all third-party providers that provide services, process, transmit, or store LAWA information or have access to LAWA systems.

Governance & Compliance

- Providers shall maintain cybersecurity policies and procedures aligned with recognized frameworks (e.g., ISO 27001, NIST CSF, CIS Controls).
- Providers shall comply with all applicable legal, regulatory, and contractual obligations.
- Providers shall identify, disclose, and manage risks associated with their third-party vendors and subcontractors involved in delivering cloud services to LAWA. Documentation of third-party risk management practices shall be provided upon request.
- A designated Information Security Officer or equivalent shall be accountable for security governance.

Access Control

- Providers shall enforce role-based access controls and the principle of least privilege.
- Providers shall enforce multi-factor authentication (MFA) for privileged and remote access.
- Access rights shall be reviewed quarterly and revoked immediately upon user termination.

Data Protection

- Confidential and sensitive data shall be encrypted at rest and in transit.
- Providers shall employ security controls to protect customer data from unauthorized access.
- Data retention shall follow contractual or regulatory requirements, with timely secure disposal.

Network & System Security

- Providers shall maintain secure configurations, firewalls, and endpoint protections.
- Security logs shall be retained for a minimum of 90 days.
- Remote connections shall use secure VPN or equivalent encryption protocols.

Vulnerability & Patch Management

- Providers shall perform quarterly vulnerability scans and remediation.
- Critical and high vulnerabilities shall be patched within industry standard (30 days and 60 days).
- Unsupported or unpatched systems are prohibited.

Incident Response

- Providers shall maintain and test an incident response plan.
- Security incidents affecting data shall be reported within reasonable time of discovery and without undue delay. Security Incident" means any confirmed breach of confidentiality, to include integrity or availability, of LAWA systems, LAWA Data, or systems or data operated or processed, by Contractor in the provision of Services to LAWA, which is due to the unauthorized or unlawful access, attack, disclosure, disruption, or denial of access and which has occurred on Provider's, and/or or any third-party systems or infrastructure that Provider uses to provide the Services, provided such third-party is under the control of Provider."
- Providers shall fully cooperate with Company incident investigations.
- Provider shall collaborate with LAWA on annual incident response tabletop exercises or simulations to validate the effectiveness of the provider's cybersecurity incident response plan. .

Continuity & Recovery

- Providers shall maintain documented Business Continuity and Disaster Recovery (BC/DR) plans.
- Recovery objectives shall meet contractual agreements.
- BC/DR plans shall be tested annually.

Personnel Security

- Providers shall perform background screening of staff in accordance with local laws.
- Providers shall conduct annual security awareness training for all staff.

Subcontractor Management

- Subcontractors engaged by the Provider shall adhere to the same security requirements.
- Providers remain accountable for subcontractor compliance.

Assurance & Audit

- LAWA may request, not more than 1 time in a rolling 12-month period, that Provider respond to a security questionnaire regarding Provider's security policies, securities procedures or security technical controls implementation as such relate to provider's Services provided to LAWA. Such questionnaire shall be reasonable in light of the nature of the services the provider is providing. Provider shall respond within a reasonable time period to such questionnaire. LAWA shall not exercise such audit right more frequently than once per twelve (12) month period.
- Any questionnaires requested, will be subject to the following terms:

  a) shall be restricted to review of provider's services provided under the Agreement;

  b) shall be subject to the confidentiality clause of the Agreement, including that LAWA will disclose to provider any third-party, which it intends to have review the questionnaire and that LAWA shall bind such third-party to a written and signed agreement with the same or substantially similar confidentiality obligations as those under the Agreement;

  c) shall be subject to a prior reasonable notice from LAWA that shall not be less than thirty (30) days, unless required sooner due to exigent circumstances;

d) shall not include either security scans or any other intrusion testing on any provider systems, without prior written consent of provider; and

e) shall be restricted to only viewing of Security Policies, Security Procedures and Security Technical Controls, which does not include production of any copies; and

f) shall be subject to full sharing of LAWA's comments with provider and sharing of such results with only such third parties with a need to know and subject to compliance with (b).

- The Provider must assist LAWA in meeting regulatory obligations and provide documentation demonstrating compliance. Regulatory authorities can audit the Provider's systems to verify compliance with these specific regulations.

I. Definitions

- Component(s) - Refers to any application, operating system, service (including but not limited to SaaS, PaaS, NaaS, IaaS), software, hardware, infrastructure, network device, server, or storage element that is part of, supports, or interacts with the proposed solution. This includes on-premises, cloud, and hybrid resources, as well as any third-party modules or integrations.
- IT - Information Technology
- IMT - Information Management and Technology Los Angeles World Airport (LAWA)
- Provider - Refers to any contractor, vendor, cloud provider, or third-party service provider delivering solutions or services to LAWA.

J. Revision History

Version	Summary of Changes	Author	Date
1.0	Initial Release	Office of Information Security	5/18/2020
1.1	Minor modification to correct grammatical errors	Office of Information Security	07/10/2020
1.2	Added Section F and G	Office of Information Security	10/28/2020
1.3	Modified Section F and G	Office of Information Security	2/3/2022
1.4	Rename Policy	Office of Information Security	3/10/2024
1.5	Updated sections F, G, added H, I	Information Security	10/14/2025