Information Technology & Telecommunications

Citywide Policy on Cloud

Final 1.0

8/22/2016

City of New York
Department of Information Technology and Telecommunications
Information Security Division

Citywide Policy on Cloud

Contents

1.0 Overview

1.1 Introduction

DoITT recognizes the value of cloud services to enhance service delivery and improve operations for the City of New York (City). Cloud services also change City operations, and there are many ways in which the cloud will affect the City's IT environment and services to the City's constituents. The goal of this policy is to facilitate diverse uses of the cloud, while ensuring optimal levels of City technology services and security.

1.2 Audience

The audience to this policy is all City of New York agencies and government entities. The entities that are considering, or may consider, the use of cloud services now or in the future must review this policy and comply with its requirements upon planning the use of any type of cloud services.

1.3 Purpose

The purpose of this policy is to ensure that all City uses of cloud services meet the City's requirements in security, performance, and evolving technical and administrative areas.

This policy outlines the ways in which cloud services interact with City IT infrastructure and services and seeks to guide City entities in the considerations that must be addressed when using cloud services. This is not a comprehensive review of all considerations, so proper diligence must be made in exploring cloud options, and DoITT serves as a resource.

1.4 Scope

This policy applies to all City of New York agencies and government entities.

This policy applies to all projects that use any type of cloud services. In particular, this policy focuses on Infrastructure as a Service (IaaS) and Software as a Service (SaaS). IaaS is commonly used to procure commoditized application hosting, such as AWS and Azure. SaaS refers to the purchase of software services hosted by the provider, such as Salesforce.com and Akamai. The policy also addresses Platform as a Service (PaaS), which provides a platform for developing, running, and managing applications. All other types of cloud services, often referred to as "X" as a service (XaaS) or "anything as a service," such as storage as a service (e.g. Google Drive), are also covered under this policy. Cloud services under the scope of this policy may be procured via contract, open source, or obtained via other any mechanism.

More detailed definitions of IaaS, SaaS, PaaS, as well as cloud computing, are defined by the National Institute of Standards and Technology (NIST) at:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

2.0 Policy

2.1 Policy Statement

City entities must inform DoITT of all uses of cloud services to ensure that proper security, legal, and operational measures are considered. City entities should inform DoITT by submitting a request through DoITT's Service Catalog.[1] DoITT will work with entities to validate that their use of cloud services is technically and administratively viable and to ensure that adequate protection measures are taken concerning City data, liability, security, and other City requirements.

All City entities seeking to select or implement a cloud service must submit their projects to DoITT as early as possible in the process, preferably at the initial planning stage. DoITT technical teams will provide guidance on the planned use of cloud. Depending on the scope, DoITT will determine whether an IT Security review is needed, advise on alternative solution pathways, if relevant, and/or provide other guidance, as applicable. Engaging with DoITT as early as possible improves DoITT's capacity to evaluate the chosen solution pathway to ensure that required information security and other City requirements can be met.

City entities must also abide by any relevant Citywide technology policies that apply to their implementation. In particular, regardless of the hosting site, City applications are subject to requirements regarding security accreditation and performance testing. In addition, City entities must adhere to information/data security regulations and requirements to ensure that they are commensurate with the classification of any data stored in the cloud.

Existing Agency Cloud Implementations

When requested, City entities will be expected to provide information to DoITT regarding all their existing cloud implementations, including those in use prior to this policy. DoITT's ultimate aim is to gather information on all cloud services used across the City in order to review issues related to security, bandwidth, and interoperability. Building and maintaining this Citywide inventory of cloud services will be critical to ensuring that the City is prepared to prevent and respond to potential security threats or compromises in a timely manner.

Sections 2.2 through 2.6 describe the types of considerations and associated reviews needed for City use of cloud services.

2.2 IaaS

All City uses of IaaS must be managed through DoITT's Self Provisioning Gateway (SPG). For IaaS cloud services not yet available through the SPG, City entities must submit their implementation plan to DoITT to determine the best approach and ensure IT Security.

[1] DoITT's Service Catalog provides information to agencies about DoITT's service offerings and enables agencies to submit service requests. City entities that do not have access to the Service Catalog should contact their Agency Relations Manager – AgencyRelations@doitt.nyc.gov.

The SPG is a web portal for New York City agencies to obtain secure provisioning of cloud infrastructure. The SPG enables authorized administrators, developers, or business users to self-provision select classes of virtual machines in DoITT's "private cloud" or in select external cloud service providers, as they become available. Virtual machines are quickly provisioned through automation. The user of the SPG is then able to use, maintain, and operate their virtual machines throughout the virtual machine's entire lifecycle.

Agencies must be on-boarded to the SPG in order to access and use it for DoITT's IaaS offerings. Agencies can request to be on-boarded by submitting a request through the DoITT Service Catalog. Once an agency has been on-boarded, approved users can access the SPG directly. Further information about DoITT's IaaS services and SPG can be found in the DoITT Self-Service Provisioning Policy. Further information about the types of virtual machines available on the SPG as well as related service information is available on the Service Catalog. DoITT IaaS offerings are currently available at no charge; however, DoITT reserves the right to charge back the cost of IaaS services to agencies in the future. Any changes in cost will be communicated to agencies and published on the SPG service page.

Entities using IaaS are responsible for working with DoITT to ensure that their use of IaaS cloud services complies with relevant Citywide IT Security policies. With DoITT support, City entities are responsible for conducting the appropriate reviews and implementing the necessary security measures required for their specific implementation. For example, in all cases that involve the handling or storage of data, IT Security policies and requirements, such as data classification and data protection, will apply.

2.3 SaaS/PaaS

All City uses of SaaS or PaaS must be reviewed and approved by DoITT IT Security prior to procurement and implementation (see section 2.5). City entities are advised to inform DoITT of their plans to leverage a SaaS or PaaS solution as soon as they have chosen the product, but at the very least, before a contract is signed. DoITT's technical team will review critical aspects of the SaaS or PaaS solution including, but not limited to, the following:

- Authentication and authorization
- Platform and hosting model (e.g. separate instance vs. multi-tenant, multi-tier)
- Data requirements
    - Classification
    - Recovery
    - Storage model
    - Retention and deletion
- Application security

2.4 Cloud Contracting

City entities must use DoITT-negotiated cloud vendor contracts, and may contract directly with external cloud providers only to obtain services that are not available through DoITT. Where DoITT's contracts do not include needed cloud services, DoITT recommends that agencies use the New York State Office of

General Services (OGS) contracts wherever possible. As with all uses of cloud services, City entities that are planning to contract directly with cloud providers should notify DoITT by submitting a request to the Service Catalog.

Entities contracting directly with cloud providers to obtain services that are not available through DoITT must maintain in their records a copy of the contract governing the use of the cloud service. This is usually a copy of the provider's service agreement or click-wrap and would otherwise not be included in the procurement document. This is true even if the cloud service is purchased using the NYS OGS or the federal General Services Administration (GSA), where the terms and conditions of the service agreement are often referenced by a hyperlink. The entity's General Counsel should review the terms of the service agreement to ensure that: a) the City is adequately protected, b) the advertised services aren't undermined by disadvantageous contract terms and hidden costs, and c) there is a binding service level agreement that includes liquidated damages.

In most cases, the service agreement will favor the provider and the City entity must negotiate for fair, reasonable and practical terms and conditions. DoITT has established a list of cloud contract considerations that must be addressed for all uses of cloud services, including data handling, security, support, and administration. This list of cloud contract considerations is included in Appendix 1. Entities must consider each topic as applicable to their specific cloud use case under negotiation. Every service agreement must include a statement disclaiming any ancillary documents or click-through agreements.

The entity should also establish clear processes and terms for on-boarding and separation assistance that guarantees the elimination of all customer data from the Cloud Service Provider ("CSP") upon separation.

A sample Cloud Service Agreement is included as Appendix 2 and can be used as a model by any City entity. DoITT's Office of General Counsel may be able to assist or advise on legal issues arising from cloud services contracting.

2.4.1 Cloud Services through City Partners

The policies stated in section 2.1 still apply in cases when a contractor or systems integrator conducts work on behalf of a City entity. If a contractor pursues a cloud solution to complete work for a City entity, that cloud solution will still need to be reviewed by DoITT to ensure it meets City technical requirements.

2.5 IT Security

DoITT IT Security works with cloud providers to ensure that cloud-based solutions are securely implemented and aligned with Citywide IT security policies. For IaaS, City entities are advised to leverage the DoITT SPG, which will provide hosting options from DoITT's private cloud as well as from external cloud service providers that have been vetted by DoITT IT Security (see section 2.2). For all other uses of cloud services that are outside DoITT's offerings, City entities must ensure that the cloud service provider is vetted and approved by DoITT IT Security. DoITT will work directly with the cloud service provider to review the provider's security certifications (e.g. compliance to FedRAMP, Service

Organization Controls, ISO standards) and/or conduct a DoITT cyber security cloud vendor assessment and/or security accreditation review.

In all cases, any applications residing in a cloud environment must go through the DoITT security accreditation review process, including those developed by, or in conjunction with, SaaS cloud providers. DoITT reserves the right to perform a cyber security assessment and/or IT audit on cloud provider environments in order to ensure that City data and systems are properly secured.

2.6 Network/Bandwidth

All City entities using cloud services outside of the DoITT SPG must account for projected bandwidth usage and ensure that they have the appropriate level of bandwidth prior to using the cloud service. If entities are unable to project their bandwidth needs, DoITT can assist the entity in completing a Network Cloud Assessment. Through this assessment, DoITT works with the City entity to determine project requirements with regard to bandwidth allocation and usage, monitoring and management support, communications, connectivity, and disaster recovery.

DoITT's Network Design and Engineering team will work with the City entity as necessary to determine the networking requirements of their project and plan accordingly. In particular, City entities should be aware that:

- The cloud vendor should confirm its ability to establish varying methods of connectivity, and provide terms associated with establishing such connectivity.
- The cloud vendor should disclose any telecommunications providers used.

3.0 Roles and Responsibilities

DoITT is responsible for ensuring that infrastructure, networks, and applications are cloud-ready and procedures are in place for connecting to the cloud. This includes maintaining the SPG, addressing IT security risks, maintaining network bandwidth, and expanding cloud offerings with selected vendors as deemed necessary. DoITT is responsible for evaluating all cloud projects (upcoming as well as existing cloud implementations) and raising issues regarding interoperability between City and cloud systems and services. DoITT serves as a resource for entities that are planning IT projects of all types, including cloud-based services.

City agencies and entities are responsible for engaging DoITT for the review of projects that will leverage cloud services. In collaboration with DoITT, agencies are responsible for ensuring the security of their data and applications and thoroughly evaluating internal and cloud options to ensure that cloud services are utilized in an efficient manner that supports the specific business need. City entities will also be expected to provide information to DoITT regarding all agencies' cloud implementations in use for DoITT review of issues related to security, bandwidth, and interoperability.

4.0 Ownership and Contact

This policy is owned by DoITT IT Security. Please contact infosecpolicy@doitt.nyc.gov with questions.

5.0 Authorship and Change History

Contributors

Geoffrey Brown, Chief Information Security Officer, Information Security – DoITT Al Frangella, Director of IT Services, Infrastructure Management – DoITT Sadia Ismat, Manager - IT Security Engineering, Information Security – DoITT Sampath Rengarajan, Senior Director of Network Architecture, Infrastructure Management – DoITT	Chad Rosenthal, Deputy General Counsel, Office of General Counsel – DoITT Don Sunderland, Deputy Commissioner, Application Development Management – DoITT Kim Truong, Policy Analyst, Office of the First Deputy Commissioner – DoITT

Change Details

Version	Change Highlights	Author(s)	Date
1.0	First publication	All contributors above	8/22/2016

6.0 APPENDIX

6.1 APPENDIX 1—Contract Considerations for Cloud Services Agreements

The public entity and the cloud service provider (CSP) must establish terms (types of service, levels of service, and cost) in each of the following areas and the CSP must demonstrate its ability to fulfill the terms, as applicable to the services under contract.

The following must be considered in all City contracts for cloud services. Adjustments can be made in accordance with the type and scope of cloud service.

DATA

1. **Backup**:
   a. In cases where backup is required, all agreements should establish service level agreements (SLAs) for the restoration process including recovery time objective (RTO) and recovery point objective (RPO), and the CSP must demonstrate its ability to meet that SLA, with penalties established for failure to meet SLA.
   b. Where backup is required, private data and its backups must be encrypted in transit and at rest.
2. **Data Retention**:
   a. Where legal mandates for data retention apply, all agreements must establish terms for preservation, retention, filtering, and retrieval. The CSP must demonstrate its ability to meet the legally mandated requirements.
   b. The CSP should define whether export will cause alteration/loss of any data or metadata.
   c. The agreement should establish terms for confirming that preservation is occurring.
   d. The agreement should establish terms for data availability (24/7/365 or other).
   e. Even where legal mandates do not apply, the CSP may not delete or remove City data without express permission of the City to do so.
3. **Business Continuity**: Where Business Continuity/Disaster Recovery (BC/DR) services are required, all agreements should establish terms for BC/DR, and the CSP must demonstrate its ability to fulfill the terms. If BC/DR is required, such requirements take precedence over the *force majeure* clause.
4. **Portability**:
   a. Where portability is required, all agreements should establish terms for portability, and the CSP must demonstrate its ability to fulfill the terms.
   b. The CSP must describe how/in what format data or applications would be returned to the customer.
   c. Where portability is required, all private data must be encrypted in transit.
5. **Data Ownership**:
   a. All data is owned exclusively by the customer agency/entity and cannot be used by the CSP for any purpose other than the services provided to the customer.
   b. The CSP should not be able to remove metadata.
   c. The CSP is given no right to use City data for any purpose other than serving the City as a customer.
6. **Data Commingling:** Data commingling should be prohibited.

IT SECURITY

Cloud providers should be able to demonstrate compliance with current Citywide Security Policies at the request of city agencies. At a minimum, they should adhere to the following:

7. **Encryption**: The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the CSP in question and approved by the Citywide Chief Information Security Officer.
8. **Incidents**:
   a. The CSP should immediately notify the customer of any breach of the security of customer data following discovery of the breach if personal or health care information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person. The CSP should also notify the agency General Counsel and the Citywide Chief Information Security Officer.
   b. The CSP should allow customers to participate in root cause analysis or agree to provide a detailed written root cause analysis for any breach.
   c. Upon City request, the CSP must supply all logs (including operating system, DBMS/database, and application logs) for the affected host machine.
   d. Terms should be set for damages in the case of harm to the customer due to security incidents.
   e. The CSP should provide a documented incident response plan.
9. **Reporting**:
   a. The CSP should provide notification of any breach and/or attempted breach.
   b. Any history of security breaches or attempted breaches must be disclosed.
   c. If the CSP is served with a warrant, subpoena or any other order or request from a government body or any other person for any records or files of customer data or metadata (as defined), the CSP will, as soon as reasonably practical and not in violation of law, deliver a copy of such warrant, subpoena, order, or request to the customer and will not comply without customer's prior written consent unless and until required to do so under applicable law.
10. **Firewalls**: The CSP should use reasonable precautions, including, but not limited to, physical, software, and network security measures; employee screening, training and supervision; and appropriate agreements with employees to:
    a. Prevent anyone other than customer or its authorized employees from monitoring, using, gaining access to, or learning the import of customer data;
    b. Protect appropriate copies of customer data from loss, corruption, or unauthorized alteration;
    c. Prevent the disclosure of customer passwords and other access control information to anyone other than authorized customer employees.
11. **Segmenting**: The CSP should implement security controls that adequately safeguard against intrusion, tampering, viruses, and other security breaches (NIST SP 800-47).
12. **Penetration Testing**: Penetration testing is required for all public-facing applications. The CSP should demonstrate the ability to conduct penetration testing and establish terms with customer for testing and cost.
13. **Vulnerability Scans**: The CSP should provide vulnerability scanning services for critical systems or systems hosting sensitive data.
14. **Vulnerabilities**: Software must be free of vulnerabilities and defects. The CSP should provide attestation by an objective third party, stating that the application has been tested for common security vulnerabilities as articulated by the "OWASP Top-10" as published by the Open Web Application Security Project (see www.owasp.org for current list of the top 10). Terms should be set for damages in the case of harm to the customer due to vulnerabilities or defects.

15. **Forensic and Investigative Response**: Chain of custody should be maintained throughout the duration of the agreement for the purposes of potential forensic or legal investigation.
16. **Security Authorizations**: The CSP should be evaluated and authorized by an independent auditor on an annual basis to ensure compliance with HIPAA/HITECH, GLB, FERPA, PCIDSS, FTC, etc. and any standards. (Note: The City cannot remove its obligation to comply with applicable statutes/standards by contracting for cloud services.)
17. **Authorization and Access**: The CSP should enforce the following IT security best practices:
    a. Least Privilege: Only authorize access to the minimum amount of resources required for a function.
    b. Separation of Duties: Functions shall be divided between staff members to reduce the threat that one person can commit fraud undetected.
    c. Role-Based Security: Access control shall be based on the role a user plays in an organization.
18. **Enhancements/Upgrades**: The CSP should notify the customer of any changes to the system, such as changes made as enhancements and upgrades, which can impact the security of the system.

SUPPORT

19. **Identity and Access Management**: The CSP should be able to support federated identity using standards approved by the New York City Chief Information Security Officer (CISO).
20. **Monitoring**:
    a. The CSP should provide information about monitoring methodology including tools and procedures.
    b. The CSP should be ITIL compliant.
21. **Service Level Agreements**: The CSP should have SLAs for incidents, with penalties if SLAs are missed.
22. **Support and Service Desk**:
    a. The CSP should define support model.
    b. The CSP should define what the customer can expect in terms of service.
    c. The CSP should be ITIL compliant.
23. **Change Management**: The CSP should provide a documented change management procedure.
24. **Upgrades**:
    a. The CSP should keep environment n-1 (not further than one version behind current) at all times.
    b. The CSP should give notification of upgrades.
    c. The CSP should outline how testing of upgrades will be performed.
25. **Performance Testing**: Performance testing is required for all public-facing applications. The CSP should demonstrate the ability to conduct performance testing and establish terms for testing and cost.
26. **Separation Assistance**: Agreement should establish clear terms and scope of separation assistance and guarantee elimination from the CSP of all customer data upon separation.

FEATURES & REQUIREMENTS

27. **Open Source**:
    a. The CSP should disclose the use of open source tools.
    b. The CSP should disclose the terms of the licensing for all open source tools used.
28. **Storage**: Storage should be configured in a high availability manner.
29. **Networking/Connectivity**:
    a. The CSP should disclose ability to establish varying methods of connectivity, and terms associated with establishing such connectivity.
    b. The CSP should disclose telecommunications providers used.

ADMINISTRATION

30. **Pricing & Costs**: All anticipated costs should be clearly outlined, agreed upon, and documented in the contract prior to work beginning. Any additional costs the CSP wishes to charge would require an amendment to the contract.
31. **Audit & Reporting**:
    a. The CSP should have the ability to deliver audit and reporting to the customer.
    b. Agreement should establish terms for the CSP to provide audit and reporting to the customer, the type of audit and reporting, frequency of audit and reporting, and delivery method.
32. **Vendor Management**:
    a. To mitigate risk, the contract should obligate the CSP to identify any functionality that is outsourced and to whom.
    b. The CSP should remain directly responsible for all aspects of complying with the terms of their contract, regardless of outsourcing.
    c. Agreements should include a clause requiring the CSP to provide notice prior to discontinuing a feature or functionality of its service, with a notification period in line with the time that it would take the agency to move to another solution.
    d. Agreements should include language addressing mergers and acquisitions, for instance: This Agreement shall be binding on the parties and their successors (through merger, acquisition or other process) and permitted assigns. Neither party may assign, delegate or otherwise transfer its obligations or rights under this Agreement to a Third Party without the prior written consent of the other party.
33. **Facilities**: All facilities holding the data should be physically located in the United States.
34. **Subcontractor(s)**: The City has legal requirements for vendor's use of subcontractors. All cloud provider subcontractors must be divulged in accordance with City regulation.
35. **Training**: The CSP is responsible for the provision of employee training and/or employee training materials.
36. **Liability and Indemnification**: The Law Department requires that there be indemnification and no limitation of liability, meaning that the contract does not place any limit on the amount of damages and costs the City can recover for a claim under the contract for personal injury, property damage or intellectual property infringement. The Law Department further recommends that confidentiality also be exempted from both the cap on consequential damages and any limitation on liability.
37. **Legal Compliance**: The CSP complies with applicable City legal mandates by the Department of Investigation and other authorities.
38. **Venue and Choice of Law:** Must be New York.
39. **Arbitration**: The City may not agree to binding arbitration.
40. **Click-throughs**: All click-through or click-wrap agreements presented to users in the course of using the Cloud services are inapplicable. Terms of contracts should be in static form. No terms should be set forth in hyperlinked websites.
41. **Unilateral Amendments:** The service agreement may only be modified by duly executed mutually agreed upon amendment. Unilateral changes and hyperlinked terms and conditions are inapplicable.

6.2 APPENDIX 2—Sample Cloud Service Agreement

The terms and conditions of this addendum ("**Rider**") supplement the EULA (End User License Agreement, as defined below) between _____, the Cloud provider ("**Licensor**"), and the City of New York (including any agency, office or commission), as licensee ("**City**" or "**Licensee**"), and are applicable to any procurement of hosted services from Licensor, including, but not limited to, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) provided to the City by Licensor or through a third-party reseller ("**Reseller**"). As used in this Rider, "party" refers to Licensor or Licensee (i.e., does not include a Reseller), individually, and "parties" means the Licensor and the Licensee, collectively.

The parties agree as follows:

1. **Additional Definitions**

"**City Data**" means information, databases, data compilations, reports, charts, graphs, diagrams, or other information created, generated or maintained by Licensor for the benefit of the City under the EULA or provided or made accessible by the City to Licensor under the EULA, including data created solely by the City's use of the Cloud Product or Software.

"**Cloud Product**" means the software-, platform-, infrastructure- or other "as a service" solution for which access is provided to the Licensee by the Licensor under the EULA.

"**EULA**" means any agreements between Licensor and Licensee that governs Licensee's use of the procured Cloud Product, and is deemed to include the terms and conditions of this Rider.

"**Privacy Laws**" means data privacy, trans-border data flow and data protection laws and regulations, including the Gramm-Leach-Bliley Act and its implementing regulations, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, the Health Information Technology for Economic and Clinical Health Act of 2009 and its implementing regulations, and U.S. State and New York City information security, data destruction and data breach notification laws and their implementing regulations.

"**Service Level Agreement**" **or "SLA"** means the term setting forth the service levels that Licensor must meet in providing the Cloud Product, including any credits to be provided for failure to meet the service levels.

2. **Order of Precedence**

This Rider takes precedence over any provision in the EULA or in any separate agreement between the City and Reseller. In the event of a conflict between this Rider and the EULA, the Rider will prevail. Defined terms in the EULA or an agreement between the City and Reseller will be given their ordinary meaning in this Rider.

3. **Term**

All terms of this Rider that should by their nature survive termination will survive, including, Sections 11 (Governing Law; Jurisdiction and Venue; Jury Waiver), 13 (City Data), and 14 (Security).

4. **Authorized Users**

The authorized user of the Cloud Product or Software is the City of New York, including its employees, authorized agents, consultants, auditors, other independent contractors and any external users contemplated by the parties. This paragraph does not modify the quantity of users licensed.

5. **Limitation Of Liability**

5.1. Subject to the provisions of Section 5.2 below, each party's aggregate liability for all claims arising out of the EULA, whether in contract, tort or otherwise, shall not exceed the greater of: (i) forty-eight (48) times the average monthly charges paid by the City to the Licensor (or Reseller, if any), calculated over the prior twelve (12) month period immediately preceding the date on which liability for the claim first arose; (ii) three times (3x) the contract value; or (iii) one million dollars ($1,000,000).

5.2. The limitation of liability set forth in Section 5.1 above will not apply to Licensor's liability arising out of any of the following: (i) Licensor's indemnification obligations under the EULA; (ii) Licensor's breach of the confidentiality provisions in this Rider; (iii) the infringement by Licensor, or any of its affiliates or subcontractors of the intellectual property of the City or of a third party; and (iv) to the extent prohibited by law.

5.3. To the extent that Licensor may be liable to the City for any action, inaction or operation of the Licensor under the EULA, including this Rider, or under statutory or common law, for which Reseller may also be liable, Licensor's and the Reseller's (if any) liabilities are joint and several, and the City is not limited in its ability to seek recourse from one or the other.

6. Warranties

6.1. SLA. Licensor represents and warrants that the Cloud Product or Software provided under the EULA will function in accordance with the agreed upon requirements and service levels. Licensor shall calculate and apply all service credits earned during a given billing period to the invoice for the following billing period. SLA claims and service credits will not be deemed to be waived by the passage of time or the City's failure to report an issue or request service credits.

6.2. Intellectual Property. Licensor represents and warrants that it has the rights necessary to license use of the Cloud Product to the Licensee in accordance with the terms of the EULA.

7. Indemnification for Intellectual Property Infringement

Licensor shall defend, indemnify and hold Licensee and its employees, officers and agents (collectively, "Indemnitees") harmless from any and all judgments, damages, liabilities, amounts paid in settlement, awards, fines, penalties, disbursements, costs and expenses (including witness fees, expert fees, investigation fees, travel expenses, bonds, the cost of establishing the right to indemnification under this Section 7, court costs and reasonable attorney's fees) to which the Indemnitees may be subjected, become liable to pay, suffer or incur in connection with any claim, allegation, suit, subpoena, action or proceeding (whether completed, actual, pending, threatened, civil, criminal, investigative, administrative, meritorious or without merit) that arises from or relates to the infringement of any copyright, trade secret, trademark, patent or other tangible or intangible property or personal right of any third party by the Licensor or its subcontractors, or by the City by its use of the Cloud Product or associated software.. Licensor shall defend, indemnify and hold the Indemnitees harmless regardless of whether or not the alleged infringement arises out of the use of the Cloud Product in a manner not expressly contemplated in the EULA or in combination with any hardware, equipment or other software not provided or authorized by Licensor. Insofar as the facts or the law relating to any claim would preclude the Indemnitees from being completely indemnified by the Licensor, the Indemnitees will be partially indemnified by the Licensor to the fullest extent permitted by the law.

8. No Additional Terms Permitted

To be valid and binding on the City, terms and conditions must bear the written signature of the Commissioner or a Deputy Commissioner of the Department of Information Technology and Telecommunications ("**DoITT**"). No online terms and conditions that are incorporated by reference in the EULA will be binding on Licensee. In addition, no shrink-wrap, click-wrap or other end user terms and conditions that are embedded in or provided with any Cloud Product are binding on Licensee, even if use of the Cloud Product or Software requires an affirmative acceptance of those terms.

9. No Portion of this Agreement may be Changed Unilaterally

No portion of the EULA, including this Rider, may be changed unilaterally. To be valid, any amendment to the EULA, including this Rider, must be in writing and signed by the parties. Any provision in the EULA to the contrary is deemed to conflict with this Rider and is be null and void.

10. Use of Third Party Providers

10.1 Licensor must identify any third party entities involved in the provision of the Cloud Product or Software and provide a copy of the agreement between the Licensor and the third party provider. The agreement must be approved in writing by the City. Any provision in the EULA to the contrary is deemed to conflict with this Rider. If Licensor proceeds with an unapproved third party provider, it will be deemed liable to the City for any third party claims to the same extent as the third party provider would be liable had it agreed to the terms set forth in this Rider.

10.2 Any subcontractor or Affiliate (as defined below) of Licensor that provides any software or services in connection with the EULA is deemed to be a subcontractor whose subcontracts must be approved in writing by the City. As used in this paragraph, "Affiliate" means any parent, subsidiary or other entity that is (directly or indirectly) controlled by, or controls, Licensor. Any provision in the EULA to the contrary is deemed to conflict with this Rider.

11. Governing Law; Jurisdiction and Venue; Jury Waiver

The laws of the State of New York, without reference to its choice of law principles, govern the EULA and any claims arising out of or relating to the EULA, its negotiation, execution, performance or breach. All disputes and controversies arising out of or relating to the negotiation, execution, performance or breach of the EULA, including this Rider, must be resolved in the New York State or federal courts in the City, County and State of New York, and each party irrevocably consents to the exclusive venue and personal jurisdiction of those courts for the resolution of disputes and waives all objections thereto. To the fullest extent permitted by law, each party irrevocably waives its right to a jury in any litigation arising out of or relating to this EULA, its negotiation, execution, performance or breach.

12. Fees.

12.1. The City is not responsible for an early termination fee.

12.2. Rates and fees may only be increased pursuant to a written amendment to this Rider that has been signed by the parties. Overage and excess usage fees are not permitted in the absence of the City's prior written agreement.

12.3. The City will not be liable for any unauthorized use, including fees and charges that may become due to Licensor as a result of that use.

12.4. The City's payment of an invoice without objection or failure to raise an objection to an invoice will not constitute a waiver of any objections to that invoice.

13. City Data

13.1. The City retains sole ownership and intellectual property rights in all City Data. Licensor does not have the right to retain any City Data other than as provided in this Rider. The EULA does not convey to either party any ownership right or license to use, sell, exploit, copy or further develop the other party's confidential information or intellectual property, including patents, copyrights, trademarks, trade names and trade secrets. The City hereby retains all right, title, and interest in and to any suggestion, enhancement request, recommendation, correction or other feedback provided to Licensor relating to the Cloud Product or Software, except that Licensor may use that information in connection with its provision of the Cloud Products or Software to the City.

13.2. Licensor shall encrypt all City Data while in transit and at rest using encryption standards and methods that are approved and recommended by the National Institute of Standards and Technology and comply with FIPS 140-2, Security Requirements for Cryptographic Modules. Licensor shall ensure that all City Data is segregated from other data maintained by Licensor, and that City Data is stored, maintained and processed on physical servers and storage devices that are dedicated to the City.

13.3. At all times during the City's agreement with Licensor, including during any suspension, and for a period of one hundred eighty (180) days after the end of that agreement, Licensor shall, at no cost to the City:

i. ensure that all City Data maintained by Licensor or its subcontractors remains immediately accessible to the City through an encrypted Internet connection;

ii. transmit encrypted City Data to the City in a format that complies with the City's Open Data Law (NYC Administrative Code §§ 23-501 et seq.), is easily usable by the City and does not include or require any proprietary software or other materials for its use; and

iii. within thirty (30) days after receiving a notice from the City's Chief Information Security Officer, copy and return City Data pursuant to the express written instructions set forth in the City's notice; unless otherwise specified in that notice, City Data must be returned on portable digital media that employs full disk encryption and the cryptographic keys must not be shipped with the City Data.

13.4. Licensor may not use, access, or perform any analytical analyses of any kind on data derived from the City's usage of the Cloud Product, whether anonymized or aggregated or both, except as agreed to in writing by the City in its discretion, or as required for the Licensor to provide Cloud Products for the City.

13.5. City Data must be located at all times in the United States, whether at rest, in transit or otherwise, except as provided in writing by the City of New York Chief Information Security Officer.

13.6. Any third party, subcontractor, or affiliate of Licensor that uses or has access to City Data is also subject to the obligations of this Sections 13 (City Data) and 14 (Security) of this Rider.

13.7. At the end of the 180-day period, or as otherwise requested by the City in writing, Licensor shall immediately destroy the City Data, including any copies, extracts, descriptions, and summaries contained in Licensor's records or systems, and provide the City with a written certification setting forth the actions taken to assure destruction. All media must be sanitized in accordance with the most recent version of NIST SP 800-00, Guidelines for Media Sanitization, or its successor publication.

14. Security

14.1 Licensor shall comply with all Privacy Laws and industry best practices (e.g., PCI DSS) ("**Industry Controls**") that are applicable to the Cloud Products, including the provision of all critical security updates and patches.

14.2 Cloud Provider shall cooperate with the City's reasonable investigation of Service issues, data security and breach issues and any suspected breach of this EULA.

14.3 Licensor shall perform a semi-annual audit of the security of the computers and the computing environment it uses in processing City Data. The audit must be performed according to ISO 27001 and SOC 2 Type II standards or the industry best-practice existing at the time of the audit, if stricter. Regardless of the standard, each audit will result in the generation of an audit report, which Licensor shall provide to the City within fifteen (15) days of performing the audit.

ACKNOWLEDGED AND ACCEPTED BY:

Licensor: _____

Name: _____

Title: _____

Date: _____

Licensee: City of New York_____

Name:_____

Title: _____

Date:_____