ATTACHMENT D

Information Security Policies

Cloud Hosting Policy

Policy #	PL-10.2.1	Effective Date	9/15/2014	Email	securityoffice@tampagov.net
Version	1.0	Contact	Zinaich, Martin	Phone	813.274.8547

Overview

Cloud and offsite hosting offer a credible alternative to traditional IT delivery models. Cloud and offsite hosting can provide benefits such as rapid delivery, enhanced scalability, agility and new funding models. This policy provides a way for the City of Tampa to utilize offsite-hosting facilities to include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) – referred to as “Cloud and Offsite Hosting Services” in the remainder of this policy.

Purpose

This policy establishes the technical terms and conditions for cloud or offsite Service Providers and services. All IT-related RFPs, Contracts, etc. must abide by this policy. These technical terms and conditions will help to protect City departments by mitigating the risks associated with entrusting the City’s data to a third party.

Scope

- This Policy is applicable to all users of the City of Tampa communications and computing resources.

- Terms and Conditions Clauses 1-10 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive.

- Terms and Conditions Clauses 11-23 are preferred but not mandatory. The applicability of each depends on the nature of engagement and will be negotiated in the final contract.

- Additional Terms and Conditions may be negotiated to meet the demands of a particular engagement, and will be identified in the final contract.

TERMS AND CONDITIONS CLAUSE 1 (MANDATORY)

The Service Provider shall have a fully implemented information security program to protect City of Tampa information assets, and provide a high-level overview of that program to the City of Tampa Information Security Office.

TERMS AND CONDITIONS CLAUSE 2 (MANDATORY)

The City of Tampa shall own all right, title and interest in its data that is related to the services provided by this contract. The Service Provider shall not access City of Tampa User accounts, or City of Tampa Data, except (i) in the course of data center operations, (ii) response to service or technical issues, (iii) as required by the express terms of the contract, or (iv) at City of Tampa's written request.

TERMS AND CONDITIONS CLAUSE 3 (MANDATORY)

Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of City of Tampa information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of City information and comply with the following conditions:

a) Personal information obtained by the Service Provider shall become and remain property of the City of Tampa.
b) At no time shall any data or processes which either belongs to or are intended for the use of the City of Tampa or its officers, agents, or employees, be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the City of Tampa.
c) The Service Provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
d) The Service Provider shall encrypt all non-public data in transit to the cloud during the life of the contract. Reference: Fla. SB. 1524 § 501.171
e) For engagements where the Service Provider stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are Social Security Number, Date of Birth, Driver's License number; passwords, financial data, and federal/state tax information.

TERMS AND CONDITIONS CLAUSE 4 (MANDATORY)

The Service Provider shall not store or transfer non-public City of Tampa data outside of the United States without the written consent of the City. This includes backup data and Disaster Recovery locations.

TERMS AND CONDITIONS CLAUSE 5 (MANDATORY)

The Service Provider shall provide written notice to the City of Tampa of any actual security breach that jeopardizes the City of Tampa data or processes. This notice shall be given to the City of Tampa within 24 hours of its discovery. Full disclosure of the jeopardized data shall be made. In addition, the Service Provider shall inform the City of Tampa of the actions it is taking or will take to reduce the risk of further loss to the City.

TERMS AND CONDITIONS CLAUSE 6 (MANDATORY)

Florida law requires public breach notification when citizen personally identifiable information is lost or stolen. Reference: Fla. Stat. § 817.5681

All communication shall be coordinated with the City of Tampa. When the Service Provider is liable for the loss, the City of Tampa shall recover all costs of response and recovery from the breach.

TERMS AND CONDITIONS CLAUSE 7 (MANDATORY)

The Service Provider shall contact the City of Tampa upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the City.   The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to the City of Tampa without first notifying the City unless prohibited by law from providing such notice.

TERMS AND CONDITIONS CLAUSE 8 (MANDATORY)

In the event of termination of the contract, the Service Provider shall implement an orderly return of City of Tampa data in a City-defined format and the subsequent secure disposal of City of Tampa data.

Suspension of services:
During any period of suspension, the Service Provider shall not take any action to erase any City of Tampa data.

Termination of any services or agreement in entirety:
In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to erase City of Tampa data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any City of Tampa data and shall thereafter, unless legally prohibited and subject to applicable law, destroy all City of Tampa data in its systems or otherwise in its possession or under its control.

Post-Termination Assistance:
The City of Tampa shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

Secure Data Disposal
When requested by the City of Tampa, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the City of Tampa.

TERMS AND CONDITIONS CLAUSE 9 (MANDATORY)

The Service Provider shall conduct criminal background checks on all staff, including sub-contractors, utilized to fulfill the obligations of the contract. If any staff being utilized to fulfill the obligations of the contract have criminal convictions or pending litigation, including but not limited to dishonesty or criminal fraud, the service provider shall notify the City of Tampa

Employment Services Manager or the City of Tampa Information Officer. The Service Provider shall promote and maintain an awareness of the importance of securing the City of Tampa’s information among the Service Provider's employees and agents.

TERMS AND CONDITIONS CLAUSE 10 (MANDATORY)

The Service Provider shall comply with the Florida public records law (Chapter 119, Florida Statutes), including Section 119.0701, Florida Statutes, if such laws are applicable to the Service Provider’s performance.

The Service Provider must manage the City of Tampa’s public records in accordance with all applicable records management laws and regulations, including those set forth by the State of Florida’s Division of Library and Information Services of the Department of State. Reference: Fla. Stat. § 119.021

TERMS AND CONDITIONS CLAUSE 11

The Service Provider shall allow the City of Tampa access to system security logs, latency statistics, etc. that affect this engagement, its data and or processes. This includes the ability for the City of Tampa to request a report of the records that a specific user accessed over a specified period.

TERMS AND CONDITIONS CLAUSE 12

The Service Provider shall allow the City of Tampa to audit conformance to the contract terms. The City of Tampa may perform this audit or contract with a third party at its discretion and at the City’s expense.

TERMS AND CONDITIONS CLAUSE 13

The Service Provider shall perform an independent audit of their data centers at least annually at their expense, and provide a redacted version of the audit report upon request. The Service Provider may remove their proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

TERMS AND CONDITIONS CLAUSE 14

Advance notice (to be determined at contract time) shall be given to the City of Tampa of any major upgrades or system changes that the Service Provider will be performing. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics and usually includes a new version number. The City of Tampa reserves the right to defer these changes if desired.

TERMS AND CONDITIONS CLAUSE 15

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the City of Tampa such that adequate protection and flexibility can be attained between the City of Tampa and the Service Provider. For example, virus checking and port sniffing – the City of Tampa and the Service Provider shall understand each other’s roles and responsibilities.

TERMS AND CONDITIONS CLAUSE 16

The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff access of customer data to that which is absolutely needed to perform job duties.

TERMS AND CONDITIONS CLAUSE 17

The City of Tampa shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Service Provider. This includes the ability for the City of Tampa to import or export data to/from other Service Providers.

TERMS AND CONDITIONS CLAUSE 18

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Service Provider. The system shall be available 24 hours per day, 365 days per year basis (with agreed- upon maintenance downtime), and providing service to customers as defined in the Service Level Agreement.

TERMS AND CONDITIONS CLAUSE 19

The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

The City of Tampa shall be notified, in advance, if any City of Tampa services or data are to be subcontracted to a third party. The Service Provider shall not subcontract any of its rights and obligations under its contract with the City of Tampa without the written consent of the City.

TERMS AND CONDITIONS CLAUSE 20

The City shall have the right at any time to require that the Service Provider remove from interaction with City data any Service Provider representative who the City believes is detrimental to its working relationship with the Service Provider. The City will provide the Service Provider with notice of its determination, and the reasons it requests the removal. If the City signifies that a potential security violation exists with respect to the request, the Service Provider shall immediately remove such individual. The Service Provider shall not assign the person to any aspect of the contract or future work orders without the City's consent.

TERMS AND CONDITIONS CLAUSE 21

The Service Provider shall provide a business continuity and disaster recovery plan upon request and ensure that the City's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) is met, as defined in the contract.

TERMS AND CONDITIONS CLAUSE 22

The Service Provider shall use web services exclusively to interface with the City's data in near real-time when possible.

TERMS AND CONDITIONS CLAUSE 23

The Service provider shall encrypt all City of Tampa non-public data that resides on any Service Provider's mobile devices during the life of the contract.

REFERENCES

Fla. Stat. § 817.5681

Fla. Stat. Chapter 119

Fla. SB. 1524 § 501.171

ISO 27002: (s)10.2.1

APPROVAL AND OWNERSHIP

Created By	Title	Date	Signature
Zinaich, Martin	ISO	9/15/2014	Martin Zinaich
Approved By	**Title**	**Date**	**Signature**
Huapert, Russell	CIO	9/15/2014	Russell Haupert

REVISION HISTORY

Version	Revision Date	Review Date	Description
1.0			Original Publication

Note: A hard copy of this document is for reference only and the latest approved version is located on the City of Tampa Intranet – Information Security Office site (Permalink)