State of Delaware
Dept. of Technology & Information
William Penn Building
801 Silver Lake Boulevard.
Dover, Delaware 19904

Phone (302) 739-9631
Fax (302) 677-7040
Email elayne.starkey@state.de.us

Date: June 14, 2011

From: Elayne Starkey
Chief Security Officer

Subject: Cloud and Offsite Hosting-- Keeping State Data Secure

To State Information Resource Managers and Information Security Officers—

A few months ago, DTI unveiled a new "Cloud First" policy, which follows in the footsteps of the Federal Government's 25 Global Technology Initiatives. Cloud Computing refers to services offered over a network and promises a credible alternative to traditional IT delivery models. Benefits include significant cost savings, enhanced scalability, agility, and rapid delivery. Conversely, entrusting infrastructure and data to a third party reduces control and introduces risks that need to be managed.

The State's **PRIVATE** cloud has been available since October 2010 and DTI is migrating customers to the virtual infrastructure. Our private cloud offering allows us to offer server replacements to our customers at a lower cost.

Cloud technology adoption rates to the **PUBLIC** cloud have been slow because of concerns around the protection of sensitive data, access control, identity management, and the lack of mature standards in the industry. We share those security concerns and are proceeding very cautiously. I am confident that, as this space matures, cloud providers will strengthen the security of their offerings. In the meantime, however, we must take an assertive stance, hold the providers accountable, and ensure security is an early consideration.

There is no need for each of our organizations to tackle cloud security independently. Start the dialogue early with your DTI Customer Relationship Specialist (CRS). Ensure that any engagement that is cloud-based or externally hosted or sends non-public data outside of the state network has been thoroughly vetted through the Business Case Process, Architecture Review Board, the iTIC, and the State's Attorney General's Office.

Attached you will find a set of contractual clauses that have been approved by DTI and the State Department of Justice. **These apply both to cloud and external hosting engagements**. The document is divided into two sections: 1) terms and conditions and 2) statement of work clauses. Contracts for cloud-based and external hosting engagements must include the non-negotiable terms and conditions. The statement of work clauses should be considered as well, and their relevance to your specific project will depend on the nature of the engagement. Examples of non-negotiable terms are:

- The State retains full ownership of the data.
- The data is not allowed to reside offshore.
- The provider must encrypt all non-public data in transit to the cloud.

- In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware assets and the subsequent secure disposal of assets.

I believe that the contractual clauses, along with assertive contract negotiation, will mitigate risks and maximize the benefits of cloud computing and offsite hosting.

Please contact my office at eSecurity.delaware.gov with any questions or concerns.

Terms and Conditions for Cloud Providers
As of May 17, 2011

No.	Doc	Item	Acknowledgement
1	T&C	Ownership of Information The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract.	
2	T&C	Privacy of Information Protection of personal privacy must be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate use of State of Delaware information at any time. To this end, the Service Provider shall comply with the following conditions: Personal information obtained by the Service Provider will become and remain property of the State of Delaware. At no time will any information, belonging to or intended for the State of Delaware, 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 State of Delaware. The Service Provider may not use any personal information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.	
3	T&C	When requested by the State of Delaware, the provider must destroy all requested data in all of its forms, disk, CD / DVD, tape, paper, for examples. Data shall be destroyed according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction must be provided to the State of Delaware.	
4	T&C	The Service Provider shall not store or transfer State of Delaware data outside of the United States.	
5	T&C	The Service Provider must inform the State of Delaware of any security breach or detection of any suspicious intrusion that is or has occurred that jeopardizes the State of Delaware data or processes. This notice must be given to the State of Delaware within 24 hours of its discovery. Full disclosure of the assets that might have been jeopardized must be made. In addition, the Service Provider must inform the State of Delaware of the actions it is taking or will take to reduce the risk of further loss to the State. If the breach requires public notification, all communication shall be coordinated with the State of Delaware.	
6	T&C	The Service Provider must encrypt all non-public data in transit to the cloud. In addition, the Service Provider will comply with the ISO/IEC 27001 standard for information security management systems, providing evidence of their certification or pursuit of certification.	
7	T&C	The Service Provider shall disclose to the State of Delaware a description of their roles and responsibilities related to electronic discovery, litigation holds, discovery searches, and expert testimonies. The provider shall disclose its process for responding to subpoenas, service of process, and other legal requests.	
8	T&C	In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware assets and the subsequent secure disposal of State of Delaware assets. **Suspension of services:** During any period of suspension, the Service Provider will not take any action to intentionally erase any State of Delaware Data. **Termination of any services or agreement in entirety:** In the event of termination of any services or agreement in entirety, the Service Provider will not take any action to intentionally erase any State of Delaware 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 State of Delaware Data and shall thereafter, unless legally prohibited, delete all State of Delaware Data in its systems or otherwise in its possession or under its control. **Post-Termination Assistance:** The State of Delaware 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 the Service Level Agreement.	
9	T&C	The Service Provider shall: 1. Ensure that State information is protected with reasonable security measures, 2. Promote and maintain among the Service Provider's employees and agents an awareness of the security needs of the State's information, 3. Safeguard the confidentiality, integrity, and availability of State information, 4. Ensure that appropriate security measures are put in place to protect the Service Provider's internal systems from intrusions and other attacks.	
10	T&C	The Service Provider shall not utilize any staff (including sub-contractors) to fulfill the obligations of the contract who has been convicted of a felony or class A misdemeanor.	
11	T&C	The Service Provider will make the State of Delaware's data and processes available to third parties only with the express written permission of the State.	
12	T&C	The Service Provider will not access State of Delaware User accounts, or State of Delaware Data, except (i) in the course of data center operations, (ii) response to service or technical issues or (iii) at State of Delaware's written request.	
		SOW	
1	SOW	The Service Provider must allow the State of Delaware access to system logs, latency statistics, etc. that affect its data and or processes.	
2	SOW	The Service Provider must allow the State of Delaware to audit conformance to the contract terms and test for vulnerabilities. The State of Delaware may perform this audit or contract with a third party at its discretion.	
3	SOW	Advance notice (to be determined at contract time) must be given to the State of Delaware of any major upgrades or system changes that the Service Provider will be performing. The State of Delaware reserves the right to defer these changes if desired.	
4	SOW	The Service Provider shall disclose its security processes and technical limitations to the State of Delaware such that adequate protection and flexibility can be attained between the State of Delaware's and the Service Provider. An example might be virus checking and port sniffing – the State of Delaware and the Service Provider must understand each other's roles and responsibilities.	
5	SOW	The Service Provider will cover the costs of response and recovery from a data breach. The State will expect to recover all breach costs from the provider.	
6	SOW	The State of Delaware will provide requirements to Service Provider for encryption of the data at rest	
7	SOW	The Service Provider shall have robust compartmentalization of job duties, perform background checks, require/enforce non-disclosure agreements, and limit staff knowledge of customer data to that which is absolutely needed to perform job duties.	
8	SOW	The Service Provider will provide documentation of internal and external security controls, and their compliance level to industry standards.	
9	SOW	The State of Delaware and the provider shall identify a collaborative governance structure as part of the design and development of service delivery and service agreements.	
10	SOW	The State of Delaware must have the ability to import or export data in piecemeal or in its entirety at its discretion without interference from the Service Provider.	
11	SOW	The Service Provider will 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 environment and/or applications must be available on a 24 hours per day, 365 days per year basis, providing around-the-clock service to customers as defined in this RFP.	
12	SOW	The web portal hosting site environment shall include redundant power, fire suppression, and 24 hours per day, 365 days per year on-site security. The hosting environment shall include redundant Internet connectivity, redundant firewalls, Virtual Private Network (VPN) services, secured remote access methods, fault tolerant internal network with gigabit Ethernet backbone, clustered central file and database servers, load balanced, application, and web servers, hardware, accelerator, three tier development environment, nightly backups, and 24x365 monitoring of all services and servers.	
13	SOW	The Service Provider shall identify all of its strategic business partners who will be involved in any application development and/or operations.	
14	SOW	The State shall have the right at any time to require that the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State will provide the Service Provider with notice of its determination, and the reasons it requests the removal. If the State 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 State's consent.	
15	SOW	The Service Provider will ensure the State of Delaware's Recovery Time Objectives (RTOs) is met.	
16	SOW	The Service Provider will provide evidence that their Business Continuity Program is certified and mapped to the international BS 259999 standard.	
17	SOW	The Service Provider shall ensure that State of Delaware backed-up data is not commingled with other cloud service customer data.	
18	SOW	**SLA/SOW - Return of Customer Data/Unique Post Termination:** The Service Provider shall make available to the State all Customer Data in a state defined format based on vendor and state platforms including: Database, O/S and physical media, along with attachments in their native format.	
19	SOW	Service Providers shall comply with and adhere to the State IT Security Policy and Standards. These policies may be revised from time to time and the Master Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available at: www.DTI.Delaware.gov	
20	SOW	The Master Contractor may deliver two copies of each software source code and software source code documentation to a State-approved escrow agent with the State's prior approval. The Master Contractor shall cause the escrow agent to place the software source code in the escrow agent's vaulted location, in Delaware, and that is acceptable to the State. Two copies of the source code shall be stored on compact discs or other media designated by the State in a format acceptable to the State, and shall be easily readable and understandable by functional analysts and technical personnel with the skill set for that type of component, subcomponent, or software code.	