



STATE OF DELAWARE
 DEPARTMENT OF TECHNOLOGY AND INFORMATION
 801 Silver Lake Blvd.
 Dover, Delaware 19904

| | | |
|------------------------|----------------------------------|---------------------------|
| Doc Ref Number: | SE-CLD-001 | Revision Number: 2 |
| Document Type: | Enterprise Policy | |
| Policy Title: | Cloud and Offsite Hosting Policy | |

| | | |
|-------------------------|---|------------------------------|
| Synopsis: | This policy provides a way for State of Delaware organizations to utilize offsite hosting facilities including cloud computing (Software as a Service, etc.) | |
| Authority: | Title 29, Delaware Code, §9004C - General powers, duties and functions of DTI "2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transport facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;" | |
| Applicability: | This Policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources. | |
| Effective Date: | 5/15/2013 | Expiration Date: None |
| POC for Changes: | Elayne Starkey, Chief Security Officer | |
| Approval By: | James Collins, Chief Information Officer | |
| Approved On: | 11/17/2014 | |



NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE
State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract # _____, Appendix _____
between State of Delaware and _____ dated _____
This document shall become part of the final contract.

| Terms and Conditions Clauses 1-13 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive. | |
|--|--|
| 1 | Data Ownership: The State of Delaware 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 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, (iii) as required by the express terms of this contract, or (iv) at State of Delaware’s written request. |
| 2 | Data Protection: 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 State of Delaware information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions: a) All information obtained by the Service Provider under this contract shall become and remain property of the State of Delaware. b) At no time shall any data or processes which either belongs to or are intended for the use of State of Delaware 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 State of Delaware. |
| 3 | Data Location: The Service Provider shall not store or transfer non-public State of Delaware data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of Delaware data remotely only as required to provide technical support. |
| 4 | Encryption: a) The Service Provider shall encrypt all non-public data in transit regardless of the transit mechanism. b) 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, financial data, federal/state tax information, and hashed passwords. The Service Provider’s encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2 , Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, they must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with the Cloud and Offsite Hosting Policy . Additionally, where encryption of data at rest is not possible, vendor must describe existing security measures that provide a similar level of protection. |
| 5 | Breach Notification and Recovery: Delaware Code requires public breach notification when citizens’ personally identifiable information is lost or stolen. Reference: 6 Del. C. § 12B-102 . Additionally, unauthorized access or disclosure of non-public data is considered to be a breach. The Service Provider will provide notification without unreasonable delay and all communication shall be coordinated with the State of Delaware. When the Service Provider or their sub-contractors are liable for the loss, the Service Provider shall bear all costs associated with the investigation, response and recovery from the breach, for example: 3-year credit monitoring services, mailing costs, website, and toll free telephone call center services. The State of Delaware shall not agree to any limitation on liability that relieves a Contractor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Contractor harmless. |

NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE
State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract # _____, Appendix ____
between State of Delaware and _____ dated _____
This document shall become part of the final contract.

| Terms and Conditions Clauses 1-13 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive. | |
|--|--|
| 6 | Notification of Legal Requests: The Service Provider shall contact the State of Delaware 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 State. The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to the State of Delaware without first notifying the State unless prohibited by law from providing such notice. |
| 7 | <p>Termination and Suspension of Service: In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State of Delaware data.</p> <p>a) Suspension of services: During any period of suspension or contract negotiation or disputes, the Service Provider shall not take any action to intentionally erase any State of Delaware data.</p> <p>b) 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 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, dispose of all State of Delaware data in its systems or otherwise in its possession or under its control as specified in section 7d) below. Within this 90 day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract.</p> <p>c) 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.</p> <p>d) Secure Data Disposal: When requested by the State of Delaware, 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 State of Delaware.</p> |
| 8 | Background Checks: The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for a minimum of 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents. |
| 9 | Data Dictionary: Prior to go-live, the Service Provider shall provide a data dictionary in accordance with the State of Delaware Data Modeling Standard . |
| 10 | Security Logs and Reports: The Service Provider shall allow the State of Delaware access to system security logs that affect this engagement, its data and or processes. This includes the ability for the State of Delaware to request a report of the records that a specific user accessed over a specified period of time. |

NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE
State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Contract # _____, Appendix ____
between State of Delaware and _____ dated _____
This document shall become part of the final contract.

| Terms and Conditions Clauses 1-13 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive. | |
|--|---|
| 11 | Contract Audit: The Service Provider shall allow the State of Delaware to audit conformance including contract terms, system security and data centers as appropriate. The State of Delaware may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days advance written notice and shall not unreasonably interfere with the Service Provider's business. |
| 12 | Sub-contractor Disclosure: 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. |
| 13 | Operational Metrics: The Service Provider and the State of Delaware shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. Examples include but are not limited to: a) Advance notice and change control for major upgrades and system changes b) System availability/uptime guarantee/agreed-upon maintenance downtime c) Recovery Time Objective/Recovery Point Objective d) Security Vulnerability Scanning |

By signing this Agreement, the Service Provider agrees to abide by all of the above Terms and Conditions.

Service Provider Name/Address (print): _____

Service Provider Authorizing Official Name (print): _____

Service Provider Authorizing Official Signature: _____

Date: _____