	Georgia Technology Authority	
Title:	**Terms and Conditions for Cloud**	
PSG Number:	**SM-14-010**	
Revision Date:	11/1/2022	**Effective Date: 4/30/2014**
Synopsis:	Terms and conditions for cloud service agreements	

PURPOSE

This standard offers a list of important components for an agency to consider inserting in a service agreement for cloud services. By no means does this list cover all situations that may be included in a service agreement; but those listed here areoften overlook ed by State agencies.

Note that non-negotiable service agreements in which terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing, but negotiated service agreements are possible, especially where a measure of customization is to be performed on the cloud service for the state agency CUSTOMER. In addition, a particular term or condition may not be worth pursuing when data involved is considered to be of LOW security characterization and there is little loss to the state if the application fails. In situations involving data impacts of MODERATE or HIGH, specific terms take on much more meaning and the Service Provider should be contractually bound (or reminded) of its shared responsibility from a statutory and regulatory standpoint.

Contractual goals (high level statements of intent for actual service agreement language) offered here are not to be considered legal advice offered by GTA, but points to be discussed within the ad hoc group of stakeholders with a final service agreement subject to the agency's legal counsel and signing authority.

Language included in a service agreement may represent some sort of managerial control desired by the agency as a protection of data, from cost escalation or from some form of loss. As with any managerial control, an agency should evaluate the cost/benefit of a proposed provision to determine if it should consider absorbing the risk that the control is designed to mitigate. Please reference the following enterprise standards:

1) For requirements to include specific terms and conditions in cloud service agreements – SA-14-003 "Requirements to Use Cloud Services", and

2) For requirements guiding determination of data impact levels - SS-08-014 "Data Categorization – Impact Level".

For ease of discussion, there are six categories of terms and conditions for service agreements between state agencies and service providers for cloud services, as follows:

- Ownership of Data and Responsibilities of Parties
- Notifications
- Audits and Reviews

- SP Staffing and Strategic Business Partners
- Operations, and
- Suspension and Termination

Stated under each category are goals for service agreement language and a brief discussion of the goals. Also included for each goal is a matrix that guides implementation of the goal according to the security categorization of the data and service.

STANDARD

Suggested Terms and Conditions for Cloud Service Agreements

(SP=Service Provider, CUSTOMER = State Agency)

(Security Categorization: LOW=L, MODERATE=M, HIGH=H)

1. Ownership of Data and Responsibilities of Parties

1.1. Goal: The State owns all non-public data

Discussion: The CUSTOMER needs to reinforce data ownership in the service agreement. The service agreement language should be specific as to the records, types of data etc. that are considered non-public data. Include statements requiring the SP to not share any Personally Identifiable Information (PII) with any other person or entity.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

1.2. Goal: SP will not access State accounts and data (list exceptions where this is permitted)

Discussion: Please be aware that the SP may require access to State data: 1) to provide the purchased service and to prevent and address technical problems, 2) as it may be compelled to disclose by law, or 3) as expressly permitted by the State in writing. Service agreement language should reinforce the goal while acknowledging the specific SP requirements for access.

Example: SP may access to State data to provide the purchased service. However, SP will not permit its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at SP's data centers in the United States. SP will permit its personnel and contractors to access State data remotely only as required to provide technical support.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

1.3. Goal: SP will not share data with its other customers, nor store data on devices with data belonging to other customers or transfer data through devices shared with other customers

Discussion: Transferring through or storing data on shared devices makes the data vulnerable to compromise or loss.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

1.4. Goal: SP will not use State data for any purpose that is not CUSTOMER related

Discussion: This provision may be included in the language establishing State ownership of data. It is reinforcing language and also intended to preclude SP sales of data or other use of the data for marketing purposes.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

1.5. Goal: Services and data shall remain in the United States

Discussion: SP will provide its services to CUSTOMER and the State's end users solely from data centers in the United States. Storage of CUSTOMER data at rest will be located solely in data centers in the United States. SP will process State data outside of SPs United States facilities only to provide services to end users of CUSTOMER located outside of the United States. The term ""data center"" applies to all SP facilities and those used by SPs contractors in which State data is processed or stored.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

1.6. Goal: Data should be encrypted for protection where the security objectives of confidentiality, authentication, non-repudiation or data integrity are categorized MODERATE or higher while the data is in motion and on all devices while at rest

Discussion: Data categorized as MODERATE or higher should be encrypted in motion as well as while at rest. If the CUSTOMER allows non-public data to be accessed by SP personnel and contractors by mobile devices, the data should be encrypted on the mobile devices. State Standard SS-08-040 requires cryptographic modules, algorithms, keys and implementations used for State information systems to meet the requirements of FIPS Special Publication 140-2 or its successors for security level 1 or higher, and to give preference to implementations validated through the Cryptographic Module Validation Program (CMVP). SP's often allow customers to select the encryption methods used.

Application of Goal According to Security Categorization:

LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

1.7. Goal: State can import/export data without interference from SP

Discussion: Typically, a customer will have such access to owned data, however, the SP may seek to limit this access if an account is suspended or terminated. Clarity in spelling out access rights as well as rights following termination or suspension is critical. (See Suspension and Termination below)

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

2. Notifications

2.1. Goal: SP will divulge to State where data is physically stored

Discussion: This goal is substantially satisfied if the SP agrees to maintain the service and data within the United States. In this case, service agreement language requiring SP divulge data location is optional.

Application of Goal According to Security Categorization:
LOW: Not Recommended
MODERATE: Optional
HIGH: Optional

2.2. Goal: SP tells when data moves and to where, i.e. relocation of storage points

Discussion: This goal is substantially satisfied if the SP agrees to maintain the service and data within the United States. In this case, service agreement language requiring SP divulge data location is optional.

Application of Goal According to Security Categorization:
LOW: Not Recommended
MODERATE: Optional
HIGH: Optional

2.3. Goal: SP notifies the CUSTOMER in the event that E-discovery, litigation hold, discovery search, or request for access by law enforcement involving access to State data is received by SP

Discussion: The SP will be bound by a legitimate request from law enforcement or courts for the above requests. The service agreement should specify how notification would take place and specific processes to be used by CUSTOMER and SP to follow up on the requests.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory

HIGH: Mandatory

2.4. Goal: SP required to cooperate and participate in servicing open records requests as passed to them by State

Discussion: As the State agency (CUSTOMER) is required by State law to cooperate and participate in servicing open records requests and the SP has physical possession of data required to service the requests, the SP must be required by service agreement language to cooperate and participate in any activities which may be necessary to service the requests also.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

2.5. Goal: State and SP each divulge security processes to the extent that State and SP understand each other's roles/responsibilities.

Discussion: State and federal program regulations, laws and IT standards require information technology providers to operate within the regulatory environment that the agency is required to operate, for example, State data privacy laws, federal regulations and laws related to Personally Identifiable Information (PII). In order to ensure that the system security is adequate and that there are no gaps in control coverage, CUSTOMER should request to review the cloud service provider's SOC audit report discussing the provider's security provisions relative to the data/system's security impact level (as defined by FISMA – Low, Moderate, High). These reports are prepared by independent auditors using audit industry accepted methodology. Comparing actual provisions to the agency's needs is a valuable tool for assessing the security of the cloud service.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

2.6. Goal: SP notifies CUSTOMER of any actual security event jeopardizing State data or process within 24 hours of discovery, what data is jeopardized in the event and what actions have been taken or will be taken to reduce further loss to CUSTOMER.

Discussion: As stated in the discussion for section 2.5 above, SP and CUSTOMER share responsibilities for security of the system and its data. The service agreement language should clarify requirements for the SP to notify CUSTOMER of security events and other pertinent information surrounding the event. Note that this is not a routine notification to be handled over the SPs web URL, but a specific expedited notification to individuals within the CUSTOMER organization or State Information Security Office.
Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

2.7. Goal: SP provides advanced notice of major upgrades, system changes and maintenance.

Discussion: Notice can be provided by direct communication of SP to Customer, or by broadcast of notice via web URL. It isn't common practice for cloud providers to push notifications to individual customers. Most SPs will typically post maintenance events to a well-known web URL, or provide the ability to see a maintenance schedule as part of an administrative portal. With this technique, the customer holds responsibility to be aware of the maintenance events. While all cloud providers we are aware of provide this visibility into their maintenance schedules, don't expect to see it called out in the contract terms.

Application of Goal According to Security Categorization:
LOW: Either method
MODERATE: Either method
HIGH: Either method

2.8. Goal: SP agrees to pay costs of response/recovery from event when SP is liable for loss

Discussion: Typical of corporate contracts, if liability for a loss can be assigned to a party to the contract the party will be expected to pay for the response and recovery from the event and possibly for punitive damages. The service agreement needs to be clear on this point as well as to any processes used to negotiate damages, monitor recovery, and costs resulting from the loss such as, but not limited to, expenses for mailing, website notifications and telephone call centers.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Recommended
HIGH: Recommended

3. Audits and Reviews

3.1. Goal: State can conduct audit for conformance to contract (State or contracted 3rd party at State expense)

Discussion: A right to audit is not something routinely offered by SPs because accommodating an audit is very expensive for both customers and providers. As a result, if a customer insists on an audit right, it is increasingly common for a service provider to charge a fee to offset costs. The state agency should ensure that audits are a necessary business requirement before asking for service agreement language to provide for audits.

Application of Goal According to Security Categorization:
LOW: Not recommended
MODERATE: Optional based on criticality of business need
HIGH: Optional based on criticality of business need

3.2. Goal: SP perform independent audit annually at their expense, State view SOC2

Discussion: Many providers will use an independent auditor to confirm their operating controls and prepare reports that attest to the control requirements of various organizations. This is done pursuant to federal laws requiring transparency in processing where financial and other types of data are involved. The state agency merely need include language in the service agreement requesting a copy of the attestment reports.

Application of Goal According to Security Categorization:
LOW: Recommended
MODERATE: Mandatory
HIGH: Mandatory

3.3. Goal: Verify that the SP managed in alignment with specific State and federal program regulations, laws and IT standards which require information technology providers to operate within the regulatory environment that the agency is required to operate (HIPAA, SOC 1/2/3 PCI DSS Lev1, ISO 27001, FedRAMP(SM), etc.)

Discussion: Many providers work to stay in alignment with a number of regulations, standards and best practices. Certifications might include one or more of the following: HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP(SM), DIACAP and FISMA, ITAR, FIPS 140-2, CSA, and MPAA

An independent auditor is normally engaged to review the SP operations and controls and attest to the design and operating effectiveness of the SPs environment.

Note that CUSTOMER can ask to review the SP SOC2 reports prior to signing a service agreement. The advantage of doing so is to compare CUSTOMER needs to the SPs controls, identify gaps in the SPs controls and then to negotiate modifications to the SPs current controls. Also, during service agreement negotiations, CUSTOMER can determine the control alignments routinely sought by the SP and include language in the service agreement requesting the reports and certifications produced by the SPsauditor.

In situations where the SP does not routinely align with CUSTOMER specified regulation, law or standard, CUSTOMER needs to negotiate in the service agreement that the SP include such alignment and request the corresponding reports and certifications.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

3.4. Goal: SP to provide timely (define term) notice of BC/DR tests and test results

Discussion: In operation, notifying CUSTOMER of scheduled outages which can impact CUSTOMER operations should be personally coordinated between SP and CUSTOMER. The service agreement should contain specific processes to be followed for notification and coordination of such testing, as well as sharing of results.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

4. SP Staffing and Strategic Business Partners

4.1. Goal: SP identify all strategic business partners in services and SP responsible for all actions of strategic business partners. Partners not permitted access to State data unless needed to perform their functions, prohibited from other usage.

Discussion: The state agency is required (enterprise standard SS-08-013) to assess and manage granting access to state systems to any third party and needs to identify all entities which will be involved in providing the contracted services. The service agreement must be specific its discussion of the responsibilities of the SP as defined in the Georgia Computer Security Act (OCGA 16-9-150) and all applicable state or federal regulation, state policies and standards. Other applicable enterprise policies and standards are PS-08-011 Third-Party Access, PS-08-014 Personnel Security, SS-08-017 Personnel Identity and Verification Screening, SS-08-013 Third –Party Security Requirements and SS-08-044 Outsourced IT Services and Third-Party Interconnections.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Mandatory
HIGH: Mandatory

4.2. Goal: SP required to conduct criminal background checks (employees, sub-contractors, etc.) and no one convicted of crime of dishonesty to work on State contract

Discussion: State Law (OCGA 13-10-91), enterprise policy (PS-08-014 Personnel Security and enterprise standards (SS-08-017Personnel Identity Verification and Screening, SS-08-013 Third –Party Security Requirements) require that individuals occupying positions of responsibility meet established security criteria and successfully pass background checks for identity and employment eligibility. The service agreement should be specific in reminding the SP of these requirements.

Application of Goal According to Security Categorization:
LOW: Mandatory
MODERATE: Mandatory
HIGH: Mandatory

4.3. Goal: SP enforce separation of job duties

Discussion: While such provisions are typically part of a review of the SPs internal controls, it may possibly be too detailed to require this in the service agreement. This should be considered optional and only pursued if deemed by the CUSTOMER to be a critical business need.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Optional
HIGH: Optional

4.4. Goal: State retains right to require SP remove from interaction w State any SP rep believed to be detrimental to working relationship. State to provide notice with reasons (see 2f above)

Discussion: This is a highly unusual requirement in a service agreement. Also, unless the individual is in a liaison or direct support position, it would be difficult for a customer to identify someone as detrimental to their operation.

Application of Goal According to Security Categorization:
LOW: Not recommended
MODERATE: Not recommended
HIGH: Not recommended

5. Operations

5.1. Goal: A "password" is the minimum access control to a cloud service and passwords must be as strong or stronger than required by State standard

Discussion: The state standard relative to passwords (SS-08-008) requires a password for systems with a security categorization of MODERATE or higher to have:

- At least 8 characters
- Characters from at least three of
    - English uppercase,
    - English lowercase,
    - Numbers, or
    - Non-alpha special characters.
- Not contain the user's name or part of the name, and
- Not contain easily accessible or guessable personal information.

Stronger mechanisms are available for access control including more stringent password schemes and/or requiring at least two of the three types of authentication:

- Potential user knowledge (such as specific passwords or PINS)
- Potential user possession (such as a private key associated with a public key certificate or an RSA token), or
- Biometric information (a person's retina scan, finger print or palm print).

Application of Goal According to Security Categorization:
- LOW: Recommended
- MODERATE: Mandatory
- HIGH: Mandatory

5.2. Goal: Include the SP's responsibilities for specified service levels, with specified calculations, escalation processes and penalties.

Discussion: Depending upon the criticality of the agency business being performed, CUSTOMER may wish to establish Service Level Agreements (SLAs) to confirm vendor

responsibilities and establish recourse should specific expected events and work level fail to be performed. For example:

- Establish a system availability SLA, based on average monthly availability, with bonuses for overachieving and increasingly steep penalties for downtime beyond the agreed level.
- Establish a system response time SLA, based on average monthly response time, with penalties for slow system performance.
- Establish an error resolution time SLA, with different windows for different severity levels (system down vs. workaround) and again with penalties for not being responsive.
- Establish a fail over window for disaster recovery SLA in the case of a catastrophic failure of the vendor's infrastructure.
- Establish an error resolution time SLA, with different windows for different severity levels (system down vs. workaround) and again with penalties for not being responsive.

Application of Goal According to Security Categorization:

- LOW: Not recommended
- MODERATE: Optional based on criticality of business need
- HIGH: Optional based on criticality of business need

5.3. Goal: SP ensures a negotiated State Recovery Time Objective (RTO)

Discussion: The SP and CUSTOMER might negotiate a Recovery Time Objective (RTO) in hours or days. The SPs specific hardware and backup and recovery processes need not be divulged, however, the RTO should be tested and demonstrated periodically during testing of the business continuity and disaster recovery plan. According to the data categorization, CUSTOMER may wish to include specific requirements for distances from primary to backup site locations, thus enhancing the potential for recovery during true catastrophic situations.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Optional based on criticality of business need
HIGH: Optional based on criticality of business need

5.4. Goal: SP comply with State website common look and feel

Discussion: This goal conflicts with the economy of the SP building a common tool to be used by many customers. However, many SPs will have a mechanism included in their services that do allow their customers some measure of modification for look and feel, such as inclusion of a logo or title. Requiring look and feel changes add to costs for development and testing.

Application of Goal According to Security Categorization:
LOW: Not recommended
MODERATE: Optional
HIGH: Optional

6. Suspension and Termination

6.1. Goal: Notification of termination of services by either party initiates an orderly return of State data in a State specified format

Discussion: A SP may move quickly to erase a customer's data in the event of the customer's suspension of service. This may be done for a number of reasons driven by service economy, such as to free up storage space. The state agency CUSTOMER needs language in the service agreement that provides a specified number of days for moving data to avoid loss of data. The CUSTOMER needs also to ensure that the period specified is sufficient to accomplish the move and that there is a plan in effect to do so.

Application of Goal According to Security Categorization:
LOW: Optional
MODERATE: Recommended
HIGH: Recommended

6.2. Goal: State should negotiate that disputed payments are exempt from triggering a service suspension for non-payment

Discussion: A disputed payment will typically not be paid by state accountants until the dispute is resolved. In the meantime, the agency does not need to be without services. One resolution in such a situation is to ensure that the service agreement includes a documented dispute procedure, with the SP agreement that when the dispute procedure is followed it will not suspend service.

Application of Goal According to Security Categorization:
LOW: Recommended
MODERATE: Recommended
HIGH: Recommended

6.3. Goal: Services and contractual rights of the State agency CUSTOMER that are defined in an original contract are preserved with any 3rd party take-over of services, or the State may terminate the agreement

Discussion: In some cases, when a service provider has sold its business to another party or the services were taken over by another party in a bankruptcy situation, the new owners initiate major operational and service changes. The State agency needs to provide some protection from this situation with service agreement language that retains its services and rights defined in the original contract, or provides for an orderly termination from the agreement with an appropriate time frame to move data in a State specified format.

Application of Goal According to Security Categorization:
LOW: Recommended
MODERATE: Recommended
HIGH: Recommended

6.4. Goal: Services to be made available to the State after receiving a notification of termination of SP services are subject to pricing process previously defined in contract

Discussion: Depending upon the criticality of the service, the State agency CUSTOMER should negotiate for at least a six (6) month period following a notification of termination of SP services to retrieve data. With a complex system, this amount of time may be required to obtain an

alternate processing capability. The SP may be willing to grant this extended period at negotiated rates for specified services.

Application of Goal According to Security Categorization:
LOW: Not recommended
MODERATE: Optional based on criticality
HIGH: Optional based on criticality

6.5. Goal: State should ask for data destruction by NIST approved methods – SP must provide a certificate of destruction

Discussion: State and federal program regulations, laws and IT standards requireinformation tec hnology providers to operate within the regulatory environment that the agency is required to ope rate. When secure data destruction by NIST approved methods are required of the State, the SP must also be required to comply.

Application of Goal According to Security Categorization:
LOW: Not Recommended
MODERATE: Mandatory
HIGH: Mandatory

6.6. Goal: SP not to erase data until after XXX days/months (defined terms)
Discussion: The State agency CUSTOMER should seek service agreement language relative to routine data erasure that supports its records retention schedule, specifying the data and record type and the length of time for its storage.

Application of Goal According to Security Categorization:
LOW: Recommended
MODERATE: Recommended
HIGH: Recommended

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Georgia Cloud First Standard (Coming Soon)

TERMS AND DEFINITIONS