**CLOUD COMPUTING CONTRACT CHECKLIST**

**for SOFTWARE AS A SERVICE**

**The following checklist contains key points, which must be considered when soliciting Cloud Computing Software as a Service (SaaS) pursuant to** [**Technology Letter 14-04**](https://cdt.ca.gov/wp-content/uploads/2017/03/TL-14-04-Cloud-Computing-Policy.pdf) **and the** [**Cloud Computing Special Provisions SaaS (SP)**](https://www.dgs.ca.gov/-/media/Divisions/PD/PTCS/OPPL/CLOUDCOMPUTINGSERVICESSPECIALPROVISIONS_18_0301.docx?la=en&hash=D15B144C86A54D492E4E19AE810F7F35EA8D171F)**. When decisions regarding these key points have been fully developed, the statement of work (SOW) can then be drafted. The SOW may modify Sections 2, 3, 6, 8 (subsections), 9, 10 and 11 of the Special Provisions. These modifications are referred to as carve outs. Definition of terms is located at the conclusion of this checklist.**

# **Data**

# **Classification and Categorization**

Classification and Categorization of the department’s Data are the critical first steps. The sensitivity of the Data helps to determine the parameters and targets for the Service Level Agreement(s) (SLAs), security, encryption, etc. Data may be separated into different levels (tiers) based on law/sensitivity/confidentiality. You must comply with [SAM 5305.5](http://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5305.5.pdf) and review this link: Classification and Categorization.

# **Basics**

Determine:

1. The format in which the State Data is to be provided to the Contactor.
2. The State’s rights to any Contractor application programming interfaces required in order to access Data.
3. What are the State’s rights to test Data access processes?
4. Roles and responsibilities for State and Contractor for installation and configuration.
5. Rights to and ownership of Data per Special Provisions #7-Rights to Data.

# **Data Breach**

The Special Provisions include a carve out for #9-Data Breach. This allows for modification of the Special Provisions if you have a business requirement. Determine:

1. Whether to treat breaches differently depending upon the Data that will be stored (public or sensitive Data, HIPAA, Personally identifiable information, Payment Card Industry, etc.).
2. What (circumstances, type of Data, etc.) should be included in the breach notifications in addition to those listed in Section 9a in the Cloud Computing Special Provisions SaaS.
3. Contractor compliance, where applicable, with Social Security Administration Document Electronic Information Exchange Security Requirement and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, security provisions in IRS Publication 1075, HIPAA, Health Information Technology for Economic and Clinical Health Act, Criminal Justice Information Services Security Policy or FedRamp (federal funds involved).

# **Locations**

The department should identify:

1. The location(s) of the Contractor Data center(s) where State Data will be processed or stored. The Special Provisions include a carve out for #6-Data Location. Will Contactor data center locations be within the parameters of your department’s Disaster Recovery Plan? The Special Provisions allow for a carve out for #10-Disaster Recovery/Business Continuity.
2. Ensure that the physical location of the data center where the Data is stored is within the continental United States, and remote access to Data from outside the continental United States is prohibited unless approved in advance by the State Chief Information Security Officer.
3. The location of the Contractor’s headquarters.
4. The distance of Contractor data center(s) from closest main internet network hub (may affect performance).
5. The Contractor’s obligation to notify the State of any location changes to Contractor’s data center(s) (that will process or store State Data), or Contractor’s headquarters.
6. Locations of State facilities where users are located (unless location is confidential).
7. What geographical limitations, if any, there will be for Data in transit.

# **Information Security**

Determineresponsibilities and obligations related to security of State information:

1. Level of Security will be driven by the department’s categorization of Data;
2. The State must determine when Data must be encrypted. Data can be encrypted:
   1. In use
   2. In transit
   3. At rest
   4. All of the above (cost consideration)
   5. Combinations of 1, 2 or 3.
3. Department must determine who will have access to the encryption key; and any encryption standards the Contractor must follow.
4. Contractor’s obligations to encrypt State Data, including level of encryption (128 bit, 256 bit, etc.). See SAM 5350.1 and SIMM 5305-A.
5. Identity and Access Management mechanisms, as provided by the Contactor, including alignment with State Identity and Access Management systems, etc.

# **Writing the SOW.**

Having made some decisions regarding your Data, the balance of this checklist will help you to write the SOW for your SaaS solicitation. Use the Cloud Computing Services Special Provisions SaaS and this guidance document for writing an SOW.

# **Service Level Agreements**

# **Basics**

Review these embedded samples of single tier and multiple tier SLAs. Each SLA should establish parameters with targets that set appropriate objectives or ranges and measure the Contractor’s performance:

1. Clear-cut and unambiguous parameters must contain performance objective(s), Data sources, Data fields’ collection times and frequency, and responsibility for Data collection, etc.
2. Will Data be placed in separate tiers (see definitions) that will use the same parameters but have different targets?
3. Aspects of performance to consider include: number of incidents, severity of incidents, time between incidents, timeliness of incident reporting, and incident resolution times.
4. Parameters must support business needs.
5. Each SLA parameter may have a single number target or a performance range and may include a minimum performance target. Failure to meet the minimum performance target may result in termination of the contract.
6. How critical is it for the service target to be achieved on specific days or dates, and/or at specific times?
7. How critical is it for the service target to occur for a given percent of time?
8. How critical is it for the service to recover from failure, and in what timeframe?
9. Consider and codify how these ranges and targets mesh with remedies or termination.

# **Terms**

The performance of the Contractor’s service must be measured to ensure quality. Examples of parameters and targets include:

1. Availability – The percentage of time the service and Data will be functional and available to the State of the total time the system is supposed to be operational (excludes agreed upon downtime). The Special Provisions allow for a carve out for #2 SaaS Availability and #3 Data Availability.
2. Times and/or days (8x5, 24x7, etc.) when SaaS is available.
3. Support – Times or days of access (8x5, 24x7, etc.), support personnel qualifications, support personnel dropped calls, etc.
4. Error Correction – The amount of time that elapses between when an error is reported to the Contractor and the time when the Contractor has corrected.
5. Latency – Determine what latency is acceptable and remedies for failure to perform.
6. “Recovery Time Objective (RTO)” – Determine the period of time within which information technology services, systems, applications and functions must be recovered following an unplanned interruption.
7. “Recovery Point Objective (RPO)” - The Recovery Point Objective is expressed as a length of time between the interruption and the most proximate backup of Data immediately preceding the interruption. The RPO must be defined in the SLA.
8. Other SLA Parameters – It is important to consider and codify any additional aspects of service that may be critical to State’s specific needs.

# **Definitions**

SLA Definitions provide additional clarifications or limitations regarding how service is calculated or measured, including what can be included or excluded. Definitions include but are not limited to:

1. Availability – The percent time that service and Data will be functional and available to the State of the total time the system is supposed to be operational (excludes agreed upon downtime The Special Provisions allow for a carve out for #2 SaaS Availability and #3 Data Availability.
2. Scheduled Maintenance – Specifically state the days and hours when the system may be unavailable for maintenance. Ensure that maintenance occurs during periods of little or no demand. This time is excluded from the calculation of Availability in the SLAs.
3. Calculations – Specific formulas, including examples, of how any given SLA is to be calculated to remove ambiguity regarding whether or not an SLA has been met.
4. Recovery Time Objective – (see Cloud Computing SaaS Special Provisions) The duration of time and service level within which service must be restored after a disruption.
5. Recovery Point Objective – (see Cloud Computing SaaS Special Provisions) The point in time to which Data must be recovered subsequent to a disaster or other disruption in service. For example, if the RPO is two hours, when a system is brought back on-line after a disaster, all Data must be restored to a point within two hours before the disaster.
6. Latency - is a measure of the speed of the system. See definitions for more detail.
7. **Reporting**

This section contains ideas for how a Contractor’s measured performance for a given SLA is reported to the State. The reporting methodology is determined by the business needs for each specific SLA. Identify whether the State or Contractor is responsible for each report. Options to consider include:

1. Reports on demand with real-time information using the Contractor’s online reports.
2. Reports published per schedule (i.e. daily, weekly, monthly, etc.).
3. Event based reporting.
4. The State’s rights to review the Contractors records related to the service level measurements.
5. **Consequences of failure to perform**

Determine remedies to be applied if the minimum SLA is not met. Some examples include:

1. Describe exigencies applied to a Contractor in the event of a missed SLA. These often take the form of financial disincentives, but there are other forms of remedies.
2. A decrease in the agreed payment for using the service, i.e., a direct financial

sanction (see Table 1).

1. A reduction in price along with additional compensation for subsequent use.
2. A reduction in usage of service.
3. Require an executive of Contractor to personally present explanations for missed SLAs to State’s management.
4. Potential disqualification of Contractor from future contracts with the State.
5. Contractor’s obligations to analyze the root cause(s) of a problem and corrective action required to prevent recurrence.
6. Contractor is required to put in place corrective actions identified as a result of the root cause analysis.
7. Remedies – Describe the effects in the event of a failure to meet an SLA performance target or other failure. Effects often take the form of financial disincentives, but there are other forms of possible remedies:
   1. A decrease in the agreed payment for using the service, i.e., a direct financial

sanction (see Table 1),

* 1. A reduction in price along with additional compensation for subsequent use,
  2. A reduction in usage of service,
  3. Require an executive of Contractor to personally present explanations for missed SLAs to State’s management,
  4. Potential disqualification of Contractor from future contracts with the State.

1. Assessing/Applying Financial exigencies – Determine:
   1. How such remedies are calculated,
   2. What portion of the total fees paid is eligible,
   3. How fees will be provided to the State (credit, refund, etc.) and
   4. Any limits on the total amounts?
2. There are other potential remedies – Consider a statement that financial exigencies are not the State’s exclusive remedy for repeated SLA failures, reserving State right to seek all damages permitted by law.
3. Repeated SLA Failures – In the event that the Contractor repeatedly fails to meet one or more SLAs (e.g., Failure to meet minimum stated SLA requirements in three (3) of any twelve (12) consecutive months), Contractor is considered to be in material breach of the agreement.
4. What event triggers a remedy? Is it a complete outage, or a specific level of performance failure? On what timeframe?
5. Who initiates the remedy? What is the State’s process? If Contractor, what are the State’s rights to audit?

Table 1

Example of Remuneration to the State for missed Availability target

|  | Target | 15% Credit | 25% Credit | 35% Credit |
| --- | --- | --- | --- | --- |
| Monthly Availability | 99.9% | 99.0% to 99.8% | 98.5% to 98.9% | 98.0% to 98.4% |

# **Contractor**

1. **Costs**

Codify costs related to continuing use of the service at current levels as well as changes in volume.

1. Costs for the State to continue using the service in subsequent renewal years. It is the State’s benefit to cap such cost at the lesser of: a specific Consumer Price Index, a set percentage, what the Contractor charges others, or the Contractor’s list price, for as long a period going forward as possible. Note: for some types of service, the Contractor’s costs decrease with time and an automatic increase would not be appropriate.
2. Cost per unit to expand current usage volume, including additional volume discount tiers, if any.
3. Cost per unit changes resulting from a decrease in State volume,
4. Minimum purchase volume commitments, if any.
5. Minimum contract periods, if any.
6. Costs for special services (Electronic Discovery, additional storage, transition services, etc.).
7. **Functionality**
8. Description of functionality being acquired, including the end result that is supposed to be achieved, as opposed to merely a product name.
9. Determine the State’s rights to replacement products providing similar functionality under a new name, if any.
10. **Outsourcing**
11. Identify any contracted functionality that Contractor outsources to a third party.
12. For any functionalities that Contractor has outsourced, Contractor must identify the third party they’ve outsourced to.
13. Ongoing responsibilities of Contractor in relation to outsourced Functionality.
14. Obligations of third parties in relation to outsourced functionality.
15. **Compliance with Laws and Standards (see Special Provisions)**

State any laws with which the Contractor is obligated to comply. Some examples include:

1. U.S. Laws (e. HIPAA, Sarbanes-Oxley, FERPA, etc.),
2. State Laws and policies,
3. Standards (ex. Payment Card Industry-Data Security Standard, etc.).
4. **Storage Limits**

Determine:

1. How much storage is included with the purchase of the cloud services?
2. Any caps on how much Data the State may store in Contractor’s cloud.
3. The cost per unit to purchase optional increased storage beyond initial buy.
4. **Technical Support**

Identify:

1. The geographic location and primary language of personnel providing support.
2. Will there be a guarantee of support availability or response time?
3. Time zone, hours for support and cost for premium (outside of normal PT) support, if any.
4. Which State end users can access support?
5. How do State end users access that support (email, phone, etc.)?
6. What is the error notification and correction process, including format and time frame(s)?
7. How do State end users access the Contractor’s services (ex. Specific web browsers, specific mobile devices, etc.)?
8. Determine the minimum timeframe within which Contractor must notify the State prior to making changes to existing technical access requirements.

# **Transition**

Eventually the contract will end. Data may have to be transitioned to another Contractor. This may require Data transition to the State and then on to another Contractor or directly from one Contractor to another. The transition period should be scheduled within the timeframe of the contract prior to conclusion. Transition will be required if the contract is prematurely terminated. The Special Provisions include carve out #8-Transition Period.

Determine:

1. How the Data will be transferred prior to conclusion of contract.
2. The length of the transition period.
3. After successful transfer of Data, how the Contractor will ensure that all Data under Contractor’s control has been destroyed or rendered inaccessible.

# **Examination and Audit**

Determine if your department’s business needs require modifications to carve out for #11-

Examination and Audit of the Special Provisions (SaaS).Specify those modifications in the SOW.

# **Definitions**

**Application programming interface** (**API**) specifies how some [software components](http://en.wikipedia.org/wiki/Software_component) should interact with each other. In practice, many times an API comes in the form of a library that includes specifications for routines, Data structures, object classes, and variables.

**Confidential Information:** Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250 et seq.) or other applicable state or federal laws. See SAM Section [5300](http://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/Sam_master_File/chap5300/5300.pdf).

**Electronic discovery** refers to discovery in civil litigation or government investigations

which deals with the exchange of information in electronic format. These Data are

subject to local rules and agreed-upon processes, and are often reviewed for privilege

and relevance before being turned over to opposing counsel.

**FERPA**

The [Family Educational Rights and Privacy Act](http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

**HIPAA**

[HIPAA](http://www.hhs.gov/ocr/privacy/) is the federal Health Insurance Portability and Accountability Act of 1996.

The primary goal of the law is to make it easier for people to keep health insurance,

protect the confidentiality and security of healthcare information.

**Latency**

In a network, latency is a synonym for delay. Latency is used in two major contexts as either one way or as a round trip. One-way latency is measured by counting the total time it takes Data to travel from its source (user) to its destination. Round-trip latency is measured by adding one-way latency from the destination to the time it takes the Data to return from the destination and arrive back at the source (user). Round trip latency can be defined and used in the SLA.

**Parameter**

In an SLA, a parameter is a system performance measurement which must be given a specific value. In Table 2, the SLA Latency is a parameter with the target of less than 50 milliseconds.

Each parameter should be defined in the SOW. Sometimes a parameters is referred to as an SLA.

Table 2

| Service Measurement | Target |
| --- | --- |
| **Latency** | <50 MS |

**Sarbanes-Oxley**

The [Sarbanes-Oxley Act](http://www.soxlaw.com/) (SOX) mandated strict reforms to improve financial

disclosures from corporations and prevent accounting fraud.

**Sensitive Information:** Information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. See SAM Section [5300](http://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/Sam_master_File/chap5300/5300.pdf). Sensitive information may be either public or confidential.

**Service Level Agreement**

Service Level Agreement or SLA is group of parameters with performance measurement targets which are used to evaluate performance. Sometimes each parameter is called an SLA.

**Target**

Each parameter must have an objective or a range of values to gauge performance.

In Table 3, the Latency parameter has a target of less than 50 milliseconds.

**Tiers for Data**

Separating Data into two or more classifications to enable more selective security/availability for more sensitive Data. For example: information already in the public domain might be categorized tier one Data and costs could be reduced since it would need no encryption. For example, highly confidential personal medical information or social security numbers could be categorized as tier two and be treated more carefully. See table 3 for examples of SLAs with tiered Data. Also see these embedded examples of single tier and multiple tier SLAs.

Table 3

|  | SLA Availability | Encryption |
| --- | --- | --- |
| Tier 1 | 99.0% | None |
| Tier 2 | 99.99% | High (e.g., 256 bit at rest, in transit and in use)\* |

\*See SAM 5350.1 and SIMM 5305-A.