110 Horizon Drive, Suite 210, Raleigh, NC 27615
919.459.2081

Service Level Agreement

Approved by the PRIA Board of Directors

July 21, 2021

www.pria.us

PROPERTY RECORDS INDUSTRY ASSOCIATION

Copyright Notice, License, Disclaimer
For
PRIA Completed Work Product

July 2021

A. **COPYRIGHT NOTICE**: Copyright © 2021 – Property Records Industry Association ("PRIA"). All rights reserved.

B. **LICENSE:** This completed PRIA work product document (the "Completed Work") is made available by PRIA to members and the general public for review, evaluation and comment only. This document is under development and not a final version.
PRIA grants any user ("Licensee") of the Completed Work a worldwide, royalty-free, non-exclusive license ("License") to reproduce the Completed Work in copies, and to use the Completed Work and all such reproductions solely for purposes of reviewing, evaluating and commenting upon the Completed Work. NO OTHER RIGHTS ARE GRANTED UNDER THIS LICENSE AND ALL OTHER RIGHTS ARE EXPRESSLY RESERVED TO PRIA. Without limiting the generality of the foregoing, PRIA does not grant any right to: (i) prepare proprietary derivative works based upon the Completed Work, (ii) distribute copies of the Incomplete Work to the public by sale or other transfer of ownership, or (iii) display the Completed Work publicly. Comments on the Completed Work must be sent to PRIA.

Any reproduction of the Completed Work shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header:

This document includes Completed Works developed by PRIA and some of its contributors, subject to PRIA License. "PRIA" is a trade name of the "Property Records Industry Association." No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee's activities and products.

C. **DISCLAIMER:** **THIS COMPLETED WORK IS PROVIDED "AS IS." PRIA AND THE AUTHORS OF THIS INCOMPLETE WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH COMPLETED WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; AND, (iii) THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA OR ANY AUTHOR OF THIS COMPLETED WORK BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS COMPLETED WORK, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA ON ANY INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF PRIA OR THE AUTHORS OR ANY STANDARD-SETTING BODY CONTRIBUTORS TO THIS COMPLETED WORK ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

Contents

Writing a Service Level Agreement (SLA)

A service level agreement is a contract between a service provider and a client. Particular aspects of the service being provided - quality, availability, responsibilities - are agreed upon between the service provider and the service user.[1] To create an effective SLA, centered on backup and restoration (not circuits or software hosting), questions need to be answered and incorporated into the contract.

1. ***Know what needs to be measured and why.***
   Quality, speed, availability, capacity, reliability, efficiency, effectiveness, timeliness, and user-friendliness are all things to measure in an SLA. These capabilities help boost customer service and satisfaction, but exactly what is being measured and how needs to be decided before creating an SLA. Make sure there is a strong relation between what is valued and what service(s) is (are) offered.

2. ***Know exactly what each Service Level measures.***
   If the exact measure of a component of an SLA is unknown, there will be gaps providers can manipulate and exploit. Define clear standards that measure each service level and provide a formula or method for calculating the end results (e.g., "if possible;" such a goal is very easy to state but very hard to measure). Service levels that cannot be measured may lead to operational deficiencies. Make sure to define specific methods for measuring each key service level. Things to remember when defining methods are accuracy, cost, and visibility.

3. ***Know the duration of the measurement period.***
   Specify timeframes in which provider performance is measured, e.g., monthly, quarterly. A short time period gives the provider a chance at more fresh starts.

4. ***What reports will the provider produce?***
   Know what reports will be given, by whom and to whom, to determine if the provider is meeting service level measurements.

5. ***What adjustments will be made if performance levels are not met?***
   Identify what adjustments will be made to the service agreement during its defined scope. For example, if the provider is to achieve 80 percent satisfaction rating in year one and then 90 percent in years two and three, what happens if those benchmarks are not met? Adjustments help ensure the provider keeps improving service.

6. ***What credits are provided in the agreement?***
   Determine what financial credits will be provided in the event the provider fails to meet service level objectives.

[1] Wikipedia

Writing an SLA for a Managed Service Provider (MSP) or a Cloud Service Provider (CSP)

Writing an SLA should take into consideration cyber-attacks on both managed solutions and cloud-based platforms. High-profile incidents indicate more cyberattacks are targeting cloud environments. In these scenarios, hackers have taken advantage of gaps in protection, shared and conflicting responsibilities, and insufficient cloud security knowledge.

- Misconfigured storage services in 93 percent of cloud deployments have contributed to more than 200 breaches over the past two years (add years?), exposing more than 30 billion records.

- Of the cloud deployments analyzed, 91 percent had at least one major exposure that left a security group wide open, in 50 percent, unprotected credentials were stored in container configuration files, which is significant because 84 percent of organizations use containers.

- Six percent of cloud-security risks are being addressed by automated technology, the report found. And, hardcoded keys are present in 72 percent of deployments[i].

Therefore, if you are contracting with an MSP or a CSP, there are additional questions to consider. Some of these questions could also be answered when defining an SLA.[2]

1. ***Is the service reliable?***
   The obvious answer from an MSP is going to be a resounding "yes!" Ask for references from businesses or groups that are of a size and business model similar to your organization. The responses and feedback could be useful in establishing an SLA with an MSP. Does the provider have existing predefined service levels, e.g., 99.9 percent is the promised availability but 96 to 98 percent is a 25 percent refund of the monthly cost and 95 percent and less is a 75 percent refund.

2. ***Does the CSP have its own data center?***
   CSPs offering data backup and disaster recovery should take the security of the physical building housing its data center seriously. Does the provider have their own data center or are they renting space in another data center? What security measures are in place if there are hardware or electrical failures? Is the data backed up both locally in the data center and in the cloud? Some providers may also provide an on premise appliance, giving three potential storage locations. Is all the data being kept within the US or is it being stored offshore in other countries?

3. ***What backup options are offered by the MSP?***
   To ensure business continuity after any disaster, make sure the MSP has both on-site and cloud-based backup options. If something happens to the data physically stored in the data center, it

[2] https://www.scmagazine.com/news/-/cloud-misconfigurations-contributed-to-more-than-200-breaches

can be accessed from the cloud-based storage and operations will be business-as-usual within moments of data loss.

4. ***What is included in the price?***

   Most cloud-based data backup and disaster recovery providers have a subscription-pricing model with clients paying a monthly or annual fee for services. Determine the specific fee/subscription costs to protect the organization from hidden fees.

   - Have a clear idea of what is truly needed because MSPs can differ on how services are provided. Some have all-encompassing services suites and others offer services á la carte.
   - Lay out what is needed from a provider and have the provider clarify the charges.
   - Don't accept one lump sum; insist on detailed line-item costs.
   - Find out if there are limits on services, e.g., the number of times a week the help desk can be called, the number of devices covered, amount of data stored.

   The object is to avoid surprise fees at the end of the service period.

5. ***What is the cost-per-megabyte of storage?***
   Evaluate requirements for storage and then determine what you need. Different tiers of storage, transfer speeds and quality of service come with different price tags. If the price is the same no matter what tier of storage is used, demand it all stay on the fastest tier so restoration comes back faster. Expect the provider to offer different options at different prices.

6. ***How fast can data be recovered?***
   Some providers are able to get an organization back up and running within a few hours, some need a few days, and some need weeks. This is dependent on the transfer rates to and from the cloud service. Restoring data (download speed) is typically more expensive than storing data (upload speed). How long can the organization operate without access to its data? The recovery solution will be built on this answer. The cost to recover data is reflected in the amount of data and the speed to recover. The organization needs to do a cost-benefit analysis to optimize both. Also ask what credits are provided if the restoration deadline is not met.

7. ***What happens if data does not come back?***
   Online backup services have technological and human errors just like any organization's environment. Something can go wrong that keeps the organization from getting all or some of its data back. Determine who is responsible for managing the storage of your data. If the data cannot be restored and the organization is fined, who is responsible for the fine? Who is accountable in the event of a legal action? Is there insurance to cover this situation? These issues must be addressed in the agreement.

8. ***What happens when the infrastructure goes down?***
   When looking at an MSP, find a provider that is prepared for disaster. The MSP should be able to describe how its disaster recovery plan (DRP), including the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), will meet your organization's requirements. There should be a recovery policy in place or a willingness to work with the organization to create a customizable plan.

9. ***What security measures are in place?***

   This question might not seem to be important at first glance, but it is. Just because the providers are offering a service does not mean they are experts or do everything right. Find out what security measures they'll take to keep the organization's data safe – including firewalls, anti-virus, and responses to threats. Find out if the organization's data is encrypted in transit and at rest. Does the provider follow industry best practices and standards? Can reports be provided for auditing purposes?

   Suggested areas to cover:

   - ***Describe the formal patch management policy and protocol.***
     Patches for all tools and systems used by the MSP should be applied in a timely manner for MSP internal operations, as well as to manage the organization's systems.
   - ***Does the MSP use multi-factor authentication (MFA) for all administrator access to the organization's systems?***
     This one measure alone could have stopped the vast majority of ransomware attacks on MSP clients' systems.
   - ***Does the MSP require use of a VPN to connect to the organization's systems?***
     Each VPN should require MFA to establish the connection and have a separate login (no shared credentials among clients) so a compromise of one client does not expose all of the others.
   - ***Does the MSP require cybersecurity training for all staff?***
     Successful phishing attacks on MSP personnel have figured in some reported incidents.
   - ***What is the MSP's password policy?***
     Strong passwords, regular changes and prohibitions against re-use are basic security. Some MSPs cut corners to make administering large numbers of clients easier.
   - ***If the organization's MSP service includes backing up systems, are those backups stored offline?***
     Regular, up-to-date backups are the best fail-safe protection against ransomware. They are ineffective if the ransomware is able to reach and encrypt the backup.
   - ***Is the MSP's network monitored for security 24/7?***
     Proactive monitoring can spot a trespasser before the intruder can execute criminal intentions.
   - ***Does the MSP have regular penetration tests on its network?***
     The MSP should undergo regular penetration testing to confirm the integrity of its security.

10. ***Does the MSP solution backup metadata, not just the files?***

    Choose a solution that backs up the organization's metadata. Metadata is essential to restore data to its original state with minimal headaches. It is a rewind solution: the organization can rewind its network and computers right back to the way they were before the data loss event occurred.

11. ***When data reaches its retention limit or it is time for the data to be deleted, is it gone from every backup and storage location?***

Proving data exists is the easy part. Proving it has been removed from every possible backup and storage location is more difficult. Find out how the MSP can prove the data is gone when it hits your organization's end-of-life policy point.

12. ***What are the steps needed to recreate the organization's data at another site in the event of a disaster that renders the organization's data servers and storage unusable?***
    Backups that cannot be restored are useless. Both the MSP and the organization should conduct periodic tests to restore data from backups to ensure the systems are working properly.

13. ***Does the provider compress and de-duplicate data to keep the cost-per-megabyte of storage down?***
    If the MSP or CSP provider online backup service charges for storage usage, backs up 50 GB of data, but is then compressing it and deduping it down to 5 GB, does the organization pay for 50 GB or 5 GB? Some services charge by the amount of data they pull from and send back to the organization's site. In this case, figure out how to reduce the data being backed up so the organization isn't paying more because multiple copies of the same file keep getting backed up.

14. ***What sort of data format conversion does the provider do?***
    Applications change over time. If retention policies demand data never be destroyed or must be kept for 10 years or more, how does the organization get its data back if it was written in an older application, or format that is no longer standard?

15. ***How can online backup service providers be changed?***
    If the organization wants to switch providers, what happens to the data currently stored with the provider? What documentation is provided to show erasure of all data once the organization leaves? Make sure there is an exit strategy in the event a better service is found or if your provider goes out of business.

16. ***What are the data ownership terms?***
    Perhaps the answer seems obvious: "You own your data." It is a crucial fact to know, especially for entities that deal with other people's personal data. Ask the MSP "what happens to the organization's data if it leaves your company?" If they try avoiding or deflecting this question, that should be a red flag. There should be no uncertain terms about who data belongs to at the end of the day, including metadata. Also ask if the MSP is planning to collect any behavioral data and, if so, what they plan to do with it. An MSP may collect this type of data to improve their services but some MSPs may sell it. Remember, it was found out that Facebook was selling personal information in 2018. They are not the only company that resells data. It is doubtful that the organization wants an MSP selling data harvested from it. The main point is that data is precious, and the organization must know what an MSP plans to do with it before handing it over.

17. ***What sort of secure media destruction is practiced?***
    This issue should be of paramount importance. Consider and ask about a situation in which a disk in the MSP's online array that holds some of the organization's data fails and the service

technician for your MSP comes and swaps out the disk, then leaves with the broken one. Broken disk or not, the organization's data is now out of the hands of the backup provider and where it ends up is unknown. If the backup provider backs up to tape, then after a certain period of time retires the media and sells it back to their media vendor to be refurbished and resold, the organization's data may very well end up in the hands of someone else. Make sure you know their policy, not just at their data center, but anywhere else the organization's data might be stored.

Summary

In summary, writing an SLA takes time and thought. Organizations need to consider many issues and be satisfied with responses to the questions before a contract is executed.