



Service Level Agreement SERVICE LEVELS

INTRODUCTION

This Attachment A sets forth certain levels of service that Provider is required to meet in performing the Services during the Term ("**Services Levels**"). As used herein "Provider" means Prevalent, Inc. and "Company" means you, the Subscriber identified in the above SaaS Subscription Agreement.

1. GENERAL PROVISIONS

1.1 Measurement and Reporting.

A. Except as otherwise agreed upon by the Parties, Provider will monitor its actual performance of the Services against the Service Levels. Provider will provide automated tools, collect and provide to Company the data reasonably made available to it by such tools, and be responsible for measuring performance against the Service Levels. Provider's failure to properly measure performance with respect to any particular Service Level for any month will be a Service Level Default with respect to such Service Level for such month.

B. Provider will provide Company with a set of hard- and soft-copy reports to verify Provider's performance and compliance with the Service Levels. Detailed supporting information for all reports will be provided to Company in spreadsheet form, or such other form as reasonably requested by Company. The raw data, detailed supporting information, and other data produced or derived from measurement of the Services will be Company Data, and may be accessed by Company on-line and in real time, where feasible, at any time during the Term.

2. DEFINITIONS

All capitalized terms used but not defined in this Attachment A have the meanings assigned to them in the Agreement. For purposes of this Attachment A, the following terms have the following meanings:

2.1 "Actual Uptime" means the aggregate amount of time within Scheduled Uptime when Services are actually available for normal business use by Company or users, as applicable (i.e., Actual Uptime = Scheduled Uptime – Outage). Services are actually available for normal business if they can be used in accordance with its intended functionality, with the required database files and tables being accessible with current data.

2.2 "Availability" means the Actual Uptime expressed as a percentage of the Scheduled Uptime (i.e., Availability % = (Actual Uptime)/Scheduled Uptime x 100%).

2.3 "Downtime" means an Outage that continues for a period of more than ten (10) minutes.

2.4 "Monthly Charge" means the amount Provider invoices Company for the Services for a given month; where Provider has quotes fees based upon a longer term the Monthly Charge will be calculated as the monthly pro rata amount of the longer term quoted..

2.5 "Outage" means any interruption of five (5) minutes or more during which ten percent (10%) or more of Company or users are unable to access the System or their access to the System is substantially impaired (including through significant logon delay).

2.6 "Service Level Default" means an occurrence of Provider's failure to meet any Service Level.

2.7 "Scheduled Uptime" means the period of time (days of the week and hours per day) the Services are expected to be available to Company for normal business use. Scheduled Uptime excludes maintenance windows for the Services.

3. SERVICE LEVEL PROCESS

3.1 Reevaluation of Service Levels. Section 5.1 of this Attachment A. identifies the Service Levels that apply during the Term, subject to the following:

A. The numerical values associated with such Service Levels (e.g., Availability of 99.9%) will be subject to Company's and Provider's mutual reevaluation three (3) months after the Effective Date. The purpose of such reevaluation is to confirm or change the numerical value based upon the average performance of Provider with respect to the applicable Service Level during such three (3) month period. Company and Provider may agree to adjust the Service Levels at this time.

B. The Parties agree that the Service Levels confirmed or changed in accordance with Section 3.1A above will not be less than those levels reasonably and consistently achievable with the systems and environments used to provide the Services if used in accordance with the practices and standards used in well-managed operations performing services similar to the Services

3.2 Additions/Modifications to Service Levels. The Parties will cooperate to identify additional Service Levels in furtherance of the objective of having a comprehensive set of Service Levels that provide a fair, accurate, and consistent

measurement of Provider's performance of the Services. In response to changes in Company's business needs or to reflect changes in or evolution of the Services, Company and Provider will, at least once per year, review and assess any changes and agree to add or substitute new Service Levels to meet such objective(s) as may be redefined from time to time during the Term.

3. SERVICE LEVELS

Provider must meet or exceed the Service Levels described in this Attachment A, including Section 5.1.

4.1 System Availability and Performance. Provider must maintain availability and performance of the System to users so as to meet or exceed the Service Levels set forth in Section 5.1.

4.2 System Capacity. Provider must provide sufficient hosting capacity to target the Service Levels, availability and performance objectives in Section 5.1. Company will work with Provider to forecast and anticipate unexpected increases in System usage due to any unusual events that could change the rate of System usage typically observed in normal site operation.

4.3 Response Time. Provider must manage equipment, bandwidth, and network response times to target Service Levels and performance objectives stated in Section 5.1.

5. SERVICE LEVEL DEFAULTS

Credits.

The SLA credits are calculated as a % of the Monthly Charge owed by Company for the month during which the Service Level Default occurs. Where Prevalent fails to attain the 99.8% service level, rather than the Service Credit set forth above Subscriber may elect to demand a pro-rata refund based upon the number of days outside of the Service the 99.8% service level and the refund will be determined on a pro rata basis using the annual Service Subscription fee stated in the Prevalent sales Quote. The refund will be paid at the end of the calendar quarter; this represents Prevalent's sole liability for that Service level breach and Subscriber's sole remedy.

5.1 SERVICE LEVELS

I. SERVICE LEVEL: SYSTEM AVAILABILITY.

Provider will provide the Application Services 24 hours per day, 365 days per year with an Availability of 99.9%, excluding scheduled maintenance, which will not be performed during Company's normal business hours of operation. Provider will provide Company with its maintenance schedule and will notify Company in advance of any non-scheduled maintenance.

II. SERVICE LEVEL: MONITORING AND RESPONSE TIME.

Provider will respond to and resolve System faults based on the severity levels detailed below. The time clock will restart any time a severity level is changed. "Response" means the time Provider takes from its receipt of a problem report until it begins work to resolve the problem. "Target Resolution" means estimated amount of time to provide a work around or other resolution.

SEVERITY LEVEL	FAULT DESCRIPTION	RESPONSE	Target Resolution
Severity 1	Production system is down, impacting all Prevalent applications.	1 hour	4 hours
Severity 2	Ability to use the Application Services, but Company operation is severely restricted and no workaround exists.	4 hours	1 business day
Severity 3	Ability to use the Application Services with faults that cause minor disruption to service.	1 business day	ASAP

III. SERVICE LEVEL: SECURITY.

A. Physical and Technical Security. Provider will provide appropriate and adequate physical and technical security for the Application Services, including, but without limitation, the following:

1. Provider will have Representatives capable of identifying, categorizing, and responding to a security incident.
2. Provider will implement a security fix across the infrastructure in accordance with Provider's regular update process.
3. Provider will promptly shut down ALL access to the System, or any component of it associated with the Application Services, responding to a request by Company's security manager.
4. Provider will not directly or indirectly subcontract, assign, or transfer, permit, or allow any portion of the Services, related support, or other activities under the Agreement offshore, meaning outside the continental United States, Canada or the United Kingdom, without the express prior written consent of the Company.
5. Provider will require all permitted subcontractors and/or third party service providers utilized either directly or indirectly by Provider in the performance of Services ("**Third Party Service Provider**") to adhere to, and with all requirements of the Agreement, including, but not limited to, the Company security requirements set forth in the Agreement.
6. Provider will conduct annual independent security reviews and audits by a reputable and nationally known independent third party audit firm to ensure that Provider is meeting all of the physical and technical security requirements of the Agreement. Provider's audit agency will prepare a written audit report detailing audit findings. Provider will not store or transmit Company Data as clear text. Provider will store and transmit Company Data only in a secure and encrypted mode.
7. Provider will institute and maintain a separation of duties between application development, quality assurance, testing, and production environments.

B. Security Event Notification.

1. If either Prevalent or Subscriber discovers or is notified of a breach or potential breach of security relating to the Subscriber Data ("Event"), (i) such party shall notify the other party of such breach or potential breach promptly but no later than 72 hours of becoming aware of the breach, and (ii) if the applicable Subscriber Data was in the possession of Prevalent or Subcontractors at the time of such breach or potential breach, Prevalent shall promptly (A) investigate and remediate the effects of the breach or potential breach, (B) provide Subscriber with information related to the breach or potential breach and coordinate with Subscriber while conducting the Prevalent's investigation; (ii) Prevalent agrees to reasonably cooperate with Subscriber to the extent Subscriber determines it is necessary to conduct its own investigation; and (iii) provide Subscriber with assurance reasonably satisfactory to Subscriber that such breach or potential breach has been remediated. Prevalent will cooperate fully with Subscriber regarding any notification for impacted individuals.

C. Prevalent implements a comprehensive backup and recovery process. More specifically, snapshots of the data ("Snapshots") are performed every 24 hours, those Snapshots are stored for 14 days.

D. Secure Audit Repository. Provider will log the following information to a secure audit repository:

- Any OS patch or OS configuration changes and the user and IP address making them;
- Account creation, deletions, and modifications (OS not application);
- Failed attempt to access data;
- Failed login;
- Start/stop of server; and
- Changes to firewall configuration files.