TIMETRAK SERVICE LEVEL AGREEMENT

This document outlines the service level agreement for USERs of TimeTrak Systems Inc. SaaS Solution. TimeTrak Systems Inc. will be referred to as “TimeTrak” throughout this agreement.

Service Level Agreement

This document contains the Service Level Agreement for TimeTrak’s SaaS Solution. Please read it carefully as this is the official agreement in force at the present time. The agreement listed below supersedes any other written document you may have prior to today's date. Exhibits to this agreement are also available highlighting additional terms. If you have questions or comments about this agreement, please do not hesitate to contact us.

This SERVICE LEVEL AGREEMENT ("Agreement" or “SLA”) shall apply to Hosted Services provided by TimeTrak. TimeTrak is committed to providing a highly available and secure network to support its USERs. Providing the USER with consistent access to Hosted Services is a high priority and is the basis for its commitment in the form of this SLA. The SLA provides certain rights and remedies in the event that the USER experiences service interruption as a result of failure of TimeTrak’s infrastructure. The overall service availability metric has consistently been 99.97%, measured on a monthly basis.

Term Definitions
For the purpose of this Service Level Agreement, the terms in bold are defined as follows:

Available or Availability
When the USER whose account is active and enabled has reasonable access to the Hosted Service, subject to the exclusions defined in Downtime Minutes below.

Total Monthly Minutes
The number of days in the month multiplied by 1,440 minutes per day.

Maintenance Time
The time period during which the Hosted Service may not be Available each month so that TimeTrak can perform routine maintenance to maximize performance, is on an as needed basis.

Downtime
The total number of minutes that the USER cannot access the Hosted Service. The calculation of Downtime Minutes excludes time that the USER is unable to access the Hosted Services due to any of the following:

(a) Maintenance Time
(b) USER’s own Internet service provider
(c) Force Majeure event
(d) Any systemic Internet failures
(e) Enhanced Services
(f) Any failure in the USER’s own hardware, software or Network connection
(g) USER’s bandwidth restrictions
(h) USER’s acts or omissions
(i) Anything outside of the direct control of TimeTrak

TimeTrak SaaS Network
The network inside of TimeTrak's SaaS border routers. All TimeTrak SaaS servers, routers and hardware are secured in locked rooms with access permitted only to appropriate IT staff.

Maintenance Notices
TimeTrak will generally communicate the date and time that it intends to make the Hosted Services unavailable at least forty-eight (48) hours in advance (or longer if practical). The USER understands and agrees that there may be instances where TimeTrak needs to interrupt the Hosted Services without notice in order to protect the integrity of the Hosted Services due to security issues, virus attacks, spam issues or other unforeseen circumstances. Below are the Maintenance Windows and their definitions:

Emergency Maintenance
These change controls happen immediately with little notification ahead of time.

Preventative Maintenance
These change controls are when we detect an item in the environment that we need to take action on, to avoid emergency change controls in the future. These change controls, if possible, will usually occur in low peak hours with peak being defined by our network metrics.

Planned Maintenance
These are change control's being done to:
1-Support on-going product and operational projects to ensure optimal performance
2-Deploy non-critical service packs or patches.
3-Periodic redundancy testing.

TimeTrak routinely does maintenance on Sunday mornings from 2AM-5AM eastern time; not every week, however TimeTrak reserves the right to take down the system during that time frame. Where possible planned maintenance will be announced at least 2-days prior; however, certain circumstances may preclude us from doing so, such as an external issue requiring a change control to TimeTrak.

System Architecture
TimeTrak's SaaS architecture is designed to maintain availability of SaaS hosted products even after physical failure, utility failure, or environmental events occur. TimeTrak's systems maintain multiple power sources with multiple points of entry, multiple WAN connections with multiple points of entry, and redundant physical and virtual layers for servers and all layers of networking.

Encryption
Secure communication of sensitive data is of the utmost importance. TimeTrak's system architecture and hosted applications utilize industry standard encryption methodologies including:
1-SSL Certificates with 2048bit digital signatures and 256bit encryption for all HTTP throughput including Web Portal and Reporting products.
2-Data transmission using custom TCP protocols allow for User Supplied Key, Independently Generated Key, and AES Standards Based Keys to encrypt data in server/client applications.

Data, Privacy, Backup and Restoration Policy
TimeTrak's SaaS data systems are designed to prevent customers from accessing physical hardware layers, hosts, or instances through the use of virtualization, Microsoft Windows user authentication, and folder/file access rights. In regards to privacy, TimeTrak requires only an employee name. In the case of payable hours transmission to payroll, some payroll structures may require an employee number to identify and match the employee on the payroll side.

1-Data redundancy

a) The first line of defense against data loss is the use of redundant arrays of independent disks (RAID). TimeTrak's physical storage layers utilize n-tier RAID configurations that maintain mirrors, stripes, and parity drives for a balanced storage array offering data integrity, performance, and unlimited growth. All parts of the RAID array are redundant and designed to maintain integrity and throughput in the case of physical failure and environmental events.

2-Backups & Restoration

a) All data is imaged daily, separated from the rest of the physical layers of the hosted system, and stored for 30 days.
b) Some data, relevant to critical aspects or time and attendance, is backed up every hour, separated from the rest of the physical layers of the hosted system, and stored for 30 days.
c) Backups are rotated and securely stored offsite, in a complete separate geographic location from the rest of the system.
d) USER Responsibility – Please note that in the case of negligence on the USER's part; for example, deletion of data - TimeTrak may/may not have the ability to restore data as data restoration is reserved for disaster recovery purposes. If data is lost due to negligence and it is determined that the data or fraction of the data can be restored, professional service fees may be applied.

USER Minimum Requirements

The required configurations USER must have to access the Hosted Services include:
1-Internet connection with adequate bandwidth
2-Internet Browser
3-Windows XP SP2 or better (Windows 7 or higher recommended)

Service Levels

Measurement

TimeTrak uses Pingdom to measure whether the Hosted Services are Available and the USER agrees that this system will be the sole basis for resolution of any dispute that may arise between the USER and TimeTrak regarding this Service Level Agreement.

Availability is calculated based on the following formula:
A = (T – M – D) / (T – M) x 100%
A = Availability
T = Total Monthly Minutes
M = Maintenance Time
D = Downtime

Availability	Credit Amount of Monthly Fee
> 97.9% but < 99.7%	5%
> 96.9% but < 97.9%	7%
< 96.9%	10%

Remedy and Procedure
The USER's remedy and the procedure for obtaining the USER's remedy in the event that TimeTrak fails to meet the Service level metrics set forth above are as follows:

To qualify for remedy:
(a) There must be a support ticket documenting the event within 24 hours of the service interruption
(b) USER account must be in good standing with all invoices paid and up to date

The USER must notify TimeTrak by email (support@timetrak.com) within five (5) business days by opening a support ticket and providing the following details.

1-Subject of email must be: "Claim Notice"
2-List the date the Downtime Minutes occurred
3-List USER's Name and E-mail address affected by Downtime Minutes
4-List an estimate of the amount of actual Downtime Minutes
5-Ticket number of the documented event

TimeTrak will confirm the information provided in the Claim Notice within five (5) business days of receipt of the Claim Notice. If TimeTrak cannot confirm the Downtime Minutes, then the USER and TimeTrak agree to refer the matter to executives at each company for resolution. If TimeTrak confirms that the Hosted Service is out of compliance with this Service Level Agreement, the USER will receive the amount of Service Level Credits set forth above for the affected Service level metric and the affected Seats for the affected month. The SLA credit will be reflected in the TimeTrak invoice to the USER in the month following TimeTrak's confirmation of the Downtime Minutes. Please note that SLA credits can only be applied to accounts that are in good standing with all invoices paid and up to date.