# ClickTime Security, Reliability, Data Integrity

***This document is an advisory notice last updated on January 15, 2019. Matters of security, web hosting, and datacenter technology change frequently so there is no guarantee that the policies and practices listed here will be in effect for any length of time.***

## *ClickTime has been protecting customers' data since 1999. It is our most important responsibility. We have always employed the latest techniques to maximize the security and availability of our systems.*

### Datacenter Physical Security:

ClickTime's datacenter is housed at a Tier 1 colocation facility. Advanced entry security, fire protection, and extensive backup power generation are provided at this facility. All access to the datacenter is controlled by 24/7 security guards and video surveillance.

Our datacenter has been granted SOC-1 certification.

### Data Security:

The ClickTime servers reside behind industry-standard routers and firewalls, which employ intrusion-protection systems and whose activities are logged. Only our customer-facing web servers have any ports exposed to the public Internet; all other system components are inaccessible to the outside world.

All servers are monitored around the clock by three independent systems. Most key system health indicators are monitored every 60 seconds. An alert is generated at any sign of service outage, intrusion, or denial-of-service and any significant events trigger automated calls to personnel on-call 24 hours a day. Sensitive customer data is encrypted at rest and in transit. All web servers and sites have SSL certificates issued by Network Solutions, verifiable by customers at any time. Traffic is encrypted with a 2048 bit key.

### RAID:

ClickTime utilizes both mechanical and solid state storage placed in RAID arrays, which can sustain the failure of multiple drive mechanisms without interrupting normal service.

### Passwords:

For customers who rely on ClickTime for password authentication, user passwords are one-way hashed prior to storage. Retrieval of clear-text passwords is not available, either to users or to ClickTime personnel.

For customers who utilize single-sign-in (SSO) systems, which is ClickTime's recommendation, passwords are maintained and managed by the external system of a customer's choosing (e.g. Okta, OneLogin, Google, Microsoft, etc.) ClickTime utilizes standards such as SAML to coordinate with external authentication sources.

### Load-balancing & Data Mirroring:

ClickTime's public web servers are fully redundant and actively load-balanced. Any individual machine can fail completely without interrupting public access to ClickTime. In addition, customer traffic is always routed to the fastest available machine.



*282 Second Street, 4th Floor*
*San Francisco, CA 94105*
*info@clicktime.com*
*www.clicktime.com*
*voice +1 (415) 684-1180*
*fax +1 (415) 684-1099*



*v3.0 20190115*

# Security, Reliability, Data Integrity

ClickTime's Primary database is mirrored to a Secondary database in real-time. The Secondary database can assume the functions of the Primary database in the event of a Primary database failure.

## On-site backup:

The ClickTime database (containing all live customer data) is backed up hourly on the same network, within the same colocation facility. Therefore, potential data loss in the event of a primary and secondary database failure is approximately 1 hour's worth of data.

## Off-site backup:

An encrypted snapshot of the ClickTime database (containing all live customer data) is sent electronically twice per day to an out-of-state datacenter. Therefore, maximum data loss in the event of a major regional disaster or multi-machine failure is 12 hours' worth of customer data entries.

## Backup rotations:

A daily snapshot of the database is committed to an archive once each day and cycled periodically to recover storage space. Depending on when we receive a request, it may be possible to retrieve or reconstruct a customer's deleted data for up to several weeks before it is overwritten. Backup retention is governed by customer contractual obligation, GDPR regulations, and ClickTime's internal policies. Customers should inquire about specific minimum and maximum backup retention periods which apply to their specific accounts.

## Secondary facilities:

In the event that ClickTime's primary physical datacenter is damaged or unavailable, ClickTime maintains a secondary "hot" datacenter on Amazon Web Services (AWS). Data retrieved from offsite backup can be restored and the secondary datacenter made live. Speed of recovery would depend on DNS propagation.

## Uptime:

Although there can be no guarantees of uptime in the future, our historical uptime as of August, 2018 is 99.9% since 2000, when statistics were first collected. (Our uptime figures are exclusive of pre-announced service outages.) Scheduled maintenance, upgrades, and feature improvements are generally announced 4 days in advance, and usually occur after 7pm Pacific Time or on a weekend. This planned downtime occurs, on average, once every eight to ten weeks.