

ClickTime has been protecting customers' data since 1999. It is our most important responsibility. We have always employed the latest techniques to protect our customers' data and maximize the 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 facility has been given SAS 70 Type II certification.

Data Security:

The ClickTime servers reside behind an industry-standard Cisco router and firewall. Only our customer-facing web servers have any ports exposed to the public Internet; all database systems are invisible to the outside world.

All servers are monitored around the clock by three redundant systems. An alert is generated at any sign of intrusion, denial-of-service, or service outage and any significant events trigger pager calls to personnel on-call 24 hours a day. Customer data files are always stored in an encrypted form. All web servers and sites have 128-bit SSL certificates issued by Network Solutions, verifiable by customers at any time.

RAID:

The ClickTime databases reside on RAID 5 and RAID 10 arrays, which can sustain the failure of any drive mechanism and immediately deploy a standby "hot spare". All front-end web server machines employ mirrored volumes for additional redundancy.

Encryption:

Passwords and other sensitive data are encrypted with AES (the Advanced Encryption Standard).

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.

The 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.

Security, Reliability, Data Integrity

On-site backup:

The ClickTime database (containing all live customer data) is backed up hourly to another machine 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.

Off-site backup:

An encrypted snapshot of the ClickTime database (containing all live customer data) is sent electronically to a storage datacenter in Massachusetts, rendering data loss in the event of a regional disaster or multi-machine failure minimal.

Additional off-site archive:

A daily snapshot of the database is committed to tape once each day. This tape is removed to an offsite location once per week and rotated. Therefore, it may be possible to retrieve a customer's deleted data after it has already been overwritten in the "fresh" backup cycle.

Secondary facilities:

In the event that ClickTime's primary datacenter is damaged or unavailable, ClickTime maintains a secondary "hot" datacenter within its own offices. Data retrieved from offsite backup can be restored and the secondary datacenter made live usually within 4 hours, depending on DNS propagation. We have a contract with an additional datacenter in Massachusetts to have machines available within 48 hours in the event of a major natural disaster in California.

Uptime:

Although there can be no guarantees of uptime in the future, our historical uptime (as of October, 2010) is over 99.9% since 1998, when statistics were first collected. (Uptime figures are exclusive of pre-announced outages.) Scheduled maintenance, upgrades, and feature improvements are announced 5 days in advance, and generally occur after 7pm Pacific Time. This planned downtime occurs, on average, once every eight to ten weeks.