PACIFIC TIMESHEET

White Paper

On-Demand Timesheet Systems and Security

How to outsource your timesheet systems safely and securely

Overview

Pacific Timesheet's robust security practices for online application service provider services fall into three areas: 1) facilities, disaster recovery and backup 2) internetworking and security 3) user account security, and 4) application security. Each area ensures significant data and security protection for customer data and proper restricted access to that data. Pacific Timesheet On-Demand Services have been provided since 1999.

Data Center Security

Backup and disaster recovery procedures

When providing On-Demand Services, Pacific Timesheet is the custodian of important customer data that must be safeguarded against the unexpected. Pacific Timesheet has in place a comprehensive disaster recovery plan to ensure that all customer data is protected should systems operations and normal database and system access need to be restored after a catastrophic event or natural disaster. Pacific Timesheet's disaster recovery plans and procedures guarantee complete recovery within 48 hours, and that data will be guaranteed up to the last business day.

There are several key elements to Pacific Timesheet's data security, back up and recovery procedures:

- Standard database mirroring techniques ensure continuous service
- Database and transaction log backups are performed stored on a daily basis. These daily backups of hosted customer data are backed up locally on tape and hard drive media.
- This data is then "pushed" electronically to secondary locations for additional safekeeping on a daily basis.
- Base functionality scripts for full database recovery are maintained at secondary and third locations.
- Communications and contingency plans include the notification and hourly updates to key customer contacts during the recovery operation.

Santa Clara Network operations center

Pacific Timesheet's disaster recovery plans and procedures are facilitated by the utilization of three facilities: its primary Network Operations Center in Santa Clara, California, its secondary data center operations in Portland, Oregon, and other hosted systems serving its IT and headquarter operations in Las Vegas, Nevada. Pacific Timesheet's key customer contact and other important customer data is maintained in a third off site data center, and its email hosting operations are hosted in a fourth off site data center to provide for continuous contact and email operations in the event of a highly localized catastrophic failure or event.

Pacific Timesheet Data Center Operation Facilities

Power distribution. Multiple 500KVA EPS6000 MGE UPS subsystems provide fully redundant power, enabling us to deliver superior IDC services in a non-stop environment backed by one of the strongest SLA's in our industry.

UPS sub-system. Pacific Timesheet's enterprise co-location services provide a non-stop Internet access infrastructure utilizing both redundant UPS subsystems and a fully automated and redundant fail-over to diesel-generator backup power. Dual and fully redundant 1.2 Megawatt, 480V CAT diesel

generators are deployed to provide non-stop power for mission-critical applications. With 2500 gallons of onsite fuel storage and contracts for continuous refilling, our non-stop IDC can run indefinitely due to an N+1 architecture implementation in all key areas.

Power generation. Pacific Timesheet's network operations center provides a non-stop Internet access infrastructure utilizing both redundant UPS subsystems and a fully automated and redundant fail-over to diesel-generator backup power. Dual and fully redundant 1.2 Megawatt, 480V CAT diesel generators are deployed to provide non-stop power for mission-critical applications. With 2500 gallons of onsite fuel storage and contracts for continuous refilling, our non-stop IDC can run indefinitely due to an N+1 architecture implementation in all key areas.

Fire suppression. Fire suppression is a very important element of IDC services. Pacific Timesheet deploys the following systems to provide the most protection from both fire and the collateral damage caused by conventional fire suppression systems.

- Fire Master (FM-200) gas-based fire suppression
- Very Early Smoke Detection Alarm (VESDA) systems
- Pre-action, double-interlocked, dry-pipe, suppression
- Below floor fire suppression

Environmental controls. Total environmental control is essential for proper operation and long life of your equipment. Electronics are susceptible to heat, humidity, and airborne dust and contaminants. These systems require precision air conditioning to prevent costly downtime. Our IDC is equipped with 175-ton Liebert HVAC and humidity control systems, raised-flooring for optimum airflow distribution and management, and constant temperature and humidity monitoring.

Facility Security. There are various levels of access and monitoring security both inside and outside of the facility. The first levels of security are proximity card access points to all external building entrances and internal IDC entrances. Additionally, all cages and secure cabinets are locked with access only by authorized customers with valid proximity cards or Pacific Timesheet support and service personnel with proximity cards. Private suites employ biometric palm scanners for secure, authenticated entrance or exit. All access at each entry or exit is monitored via video recording and proximity card reader logs. All walls of the IDC are reinforced barrier design with no windows. A raised-floor IDC design allows all primary power, Ethernet, Telco, and carrier cables and feeds to be delivered to their destination completely under the floor and securely out of harms way. The entire exterior and interior of the facility is also monitored by digital video surveillance cameras located throughout the facility premises. Man-trap (two secure and monitored doors) entrances are also employed at both the front and rear entrances of the IDC.

IDC Specifications. From high-speed dedicated access solutions to high-end managed co-location solutions, our primary IDC is truly a state-of-the-art carrier-class facility providing outstanding reliability,

availability, and scalability. Our Class-A IDC provides fully redundant power, fully redundant carrier connectivity, and fully redundant upstream IP connectivity, environmental controls, diverse fire-suppression systems, video surveillance, secure access, and a carrier-neutral philosophy enabling us to deliver superior IDC services backed by one of the strongest SLA's in our industry.

Internetworking and Security

All Pacific Timesheet production On-Demand Services systems are secured by SSL and https. Secure Sockets Layer uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL

Pacific Timesheet's firewall security manages internet traffic with various rules to restrict access to only customer requests. Pacific Timesheet application software, middleware, and databases are never exposed directly to the internet, Timely service patch updates, software and system upgrades ensure that new or potential security threats are managed effectively and ensure continuous On-Demand service operations.

User Account Security

Pacific Timesheet On-Demand Services applications have several account security features that restrict access to authorized and authenticated users.

Standard security features

Disable user's account after N failed logon attempts

Another standard feature that is enabled globally, the system will disable a user's account after N failed attempts and be permanently locked out of the system until a system administrator resets the password. The user receive an error message instructing them that they have too many failed login attempts and that their account has been inactivated. They are also instructed to contact their system administer to reactivate the account. When a user's account is inactivated both their login and passwords are not active.

Require new users to change their password on first logon

This standard feature, that is enabled globally, is applied when a user is logging in for the first time to the system is prompted to change his password.

Require users to change their password after it is reset by an administrator or the system

This standard feature, that is enabled globally, is applied after a system administrator or system has reset the user's password. The user is then prompted to change this password as if they were logging in for the first time.

Require users to change their passwords after N days

This standard feature, that is enabled globally, is often applied to force users to change their passwords every 60 or 90 days.

Don't allow passwords shorter than N characters

This standard feature, that is enabled globally, restricts users from setting passwords with less than a prescribed number of characters.

Require passwords to have one alpha and one numeric and/or special character
Another standard feature that is enabled globally, users can be required to include at least one alpha and one numeric character in their password.

Don't allow passwords to be changed unless at least N days old
Another standard feature that is enabled globally, users can be required to keep passwords for a designated number of days before changing them.

Remember user's last N passwords, and require new passwords to be different
Another standard feature that is enabled globally, the system will remember up to the last N passwords used by a user and can require new passwords to be different from the last N passwords.

Application Security

Pacific Timesheet's extensive application security includes group security, work item security and roles based security features that user restrict user access in a variety of ways.

Group security

Group security features include group hierarchies, group assignments, and group reporting access that limit users to group data access defined by their system role for that group.

Roles-based security

When combined with group security and project security restricts access of users and other key roles to various group or project data. Roles can enable or disable certain rights such as the ability of a user to assign or unassign users or projects. Administrative rights can be centralized or decentralized.

Work Item security

Projects organized with a work breakdown structure (WBS) can have secured or restricted access at any of their levels.

Administrative security

Administrative security can be assigned by group, project, and/or role in a variety of configurations depending up an organization's policies, rules and structure.

Contacting Pacific Timesheet

Contact a Pacific Timesheet representative to receive a full demonstration of our products and services.

Headquarters:
5348 Vegas Drive
Las Vegas, NV 89108
866-416-2061