



Workstream Hosting Service Overview



TABLE OF CONTENTS

WHY USE A HOSTING SERVICE?	3
SARBANES-OXLEY (SOX) COMPLIANT	3
SAS70 TYPE I CERTIFIED	3
TOTAL SECURITY MANAGEMENT	4
BACKUPS	4
FIREWALLS	4
SERVERS	5
BUSINESS CONTINUITY SOLUTION INCLUDED	5
NETWORK AVAILABILITY	5

Why use a Hosting Service?

Using a hosting service in today's fast-paced world just makes practical business sense. First, you have complete control over your application instance. Second, with a hosting service you do not have the costs associated with acquiring, running and staffing your own systems. You also do not have tasks such as daily backups to contend with. Third, we provide for all of your security needs, from physical security (often forgotten), to network security to site security.

Workstream Hosting Service provides a secure, fault tolerant, scalable framework for customer deployments, complete with a Service Level Agreement (SLA). With a high-availability network, comprehensive security, business continuity provided through SunGard, and a SAS70 certified data center, the Workstream hosting solution ensures not just excellent HR applications but world-class hosting.

Sarbanes-Oxley (SOX) Compliant

Workstream has completed its testing requirements and is deemed in compliance with Section 404 of the Sarbanes-Oxley Act of 2002. Meeting with the highest financial standards, Workstream has been working through a certification process with its auditors PricewaterhouseCoopers over the past year. The report from the independent auditors may be seen in our 2005 Annual Report.

SAS 70 Type I Certified

Workstream has passed SAS 70 Type I certification. KPMG an AICPA certified firm completed the audit and certified Workstream SAS 70 compliant as of May 2006. The controls that Workstream audited against are:

- Change Management
- Logical Access and Security
- Logical Security
- Physical Security
- Environmental Controls
- Event Management and Problem Resolution
- Network and System Monitoring
- Backup of Systems and Customer Data
- Data Transmissions
- Computer Operations

Total Security Management

The Workstream data center maintains state-of-the-art facilities to ensure both the security of all client data and 24/7/365 application availability. The base level physical security includes a UPS with a 36-hour diesel generator, complete fire suppression system, multiple cooling units, as well as temperature and water sensors in the data center. Our data center also has raised floors for secure routing of power and data cables and is monitored by a third party company which ensures that potential environmental issues are addressed immediately.

Physical access control for the Workstream data center is provided by Workstream and our landlord. This facility is monitored 7/24/365 for all access and is restricted to authorized system administrators. There are five levels of secure access to client data including:

- Building access
- Floor access
- Facility access
- Data center facility access
- System hardware access

In addition to the physical security measures described above, Workstream maintains complete data and application-level security that leverages the most current technologies including:

- Hardened operating system and application builds
- Fully managed firewalls & virus protection
- 128-bit encryption for privacy
- Third Brigade Deep Security - advanced host intrusion detection & intrusion prevention
- Regular security scans and vulnerability testing
- External penetration testing and audits to validate

Backups

Workstream provides automated daily backup and long-term offsite storage of our customers' data. Offsite tapes are protected from fire, flood and other natural disasters. Workstream uses Iron Mountain, a bonded 3rd party service provider specializing in electronic tape storage. The tapes destined for offsite are collected on a daily basis by a secure carrier. Our backup media is accessible only by authorized individuals.

Firewalls

To ensure that all customer information is secure, the Workstream hosting network is physically separated from the Internet via firewalls. All access to these firewalls is limited to members of the Workstream Operations and Security teams. In addition, a highly secure firewall configuration allows only traffic destined for the ports required by the application to be accessible externally. Finally, Workstream's firewalls are configured to drop and log any unusual network activity.

Servers

Workstream is able to provide consistently high levels of service regardless of the traffic situation. Our Internet connectivity is provided by three vendors; Allstream, Bell and Sprint and is configured via BGP running on Cisco equipment. We disable all unnecessary services on our servers and verify all necessary components have the latest patches installed during the initial configuration. All patches are first tested in the QA environment before being deployed in production. Workstream subscribes to daily vulnerability reports from various security agencies.

Business Continuity Solution Included

Workstream maintains a comprehensive business continuity/disaster recovery plan as part of its hosting service. This plan includes both daily backups of all customer data with off-site storage and complete disaster recovery with SunGard.

Workstream has signed a long-term agreement with SunGard, (www.sungard.com) a leader in providing disaster recovery services. The primary recovery site is located in Toronto, Ontario with the secondary site situated in Philadelphia. The agreement gives Workstream access to any of the other 20+ recovery sites in North America. In addition SunGard can provide onsite replacement or augmentation during an event. The first phase of system testing was completed in December, 2005. Complete implementation is planned for early 2007.

Network Availability

Workstream ensures the highest standards for network availability with high-capacity circuits, burst capability, and failover circuits.

We utilize proactive monitoring/resolution, and WAN performance tracking. Our enhanced burst network capacity includes 2 X 15 50MB burstable circuit and 1 X 10 40MB burstable circuit. In addition, the Workstream data center has dual failover circuits – one through an Allstream Dual Multi-path connection and another through Sprint.

Workstream uses Symantec software to protect against viruses/worms and Trojan attacks. Symantec Manager is utilized to automatically push the latest anti-virus definitions to the servers and workstations throughout the environment. We have also implemented Third Brigade Deep Security, an advanced intrusion prevention system. This software is used to enforce comprehensive security policies that proactively protect sensitive data, applications, and hosts by monitoring incoming and outgoing network traffic for protocol deviations or contents that might signal an attack. When necessary, Deep Security intervenes and neutralizes the threat by either blocking or correcting the traffic.

About Workstream

Workstream provides enterprise workforce management solutions and services that help companies manage the entire employee lifecycle – from recruitment to retirement. Workstream's TalentCenter provides a unified view of all Workstream products and services including Recruitment, Benefits, Performance, Compensation, Development and Transition. Access to TalentCenter is offered on a monthly subscription basis under an on-demand software delivery model to help companies build high performing workforces, while controlling costs. With 9 offices across North America, Workstream services customers including Chevron, The Gap, Home Depot, Kaiser Permanente, Motorola, Nordstrom, Samsung, Sony Music Canada, VISA and Wells Fargo. For more information visit www.workstreaminc.com or call toll free 1-866-470-WORK.



U.S Headquarters
2600 Lake Lucien Drive
Suite 410
Maitland, FL 32751
Toll free: 866 470 WORK
Fax: 407 475 5500
www.workstreaminc.com