NaviSite®

DATA SHEET

NaviSite's SSAE 16 Compliant Data Centers

Benefits

- Meets and Exceeds Internationally Recognized Auditing Standard
- Strong SLAs
- Physical Security Controls
- Logical Security Controls
- Full Monitoring, Event Resolution, and Triggering
- Redundant Anti-Virus Protection
- Redundant System Backup

NaviSite's SSAE 16 compliant data centers meet the highest security standards for data and application integrity. SSAE 16 compliance is an internationally recognized auditing standard of the American Institute of Certified Public Accountants and is further assurance that NaviSite follows stringent controls and safeguards. With n+1 redundancy in all systems, NaviSite offers the strongest Service Level Agreements (SLAs) in the industry.

HIGHLY CONTROLLED SSAE 16 ENVIRONMENT

Section 404 of the Sarbanes-Oxley Act of 2002 requires public companies to demonstrate and maintain effective corporate controls across a variety of business functions. Many companies are spending a significant amount of money to institute these controls and reorganize their business processes accordingly. To help our customers in this arena, NaviSite has achieved and maintains SSAE 16 compliance, providing independent assurance that NaviSite has demonstrated adherence to rigorous corporate controls in a variety of areas.

More importantly, with our SSAE 16 Environment Upgrade, NaviSite extends the benefits of our SSAE16 compliance to our customers, enabling them to use NaviSite's SSAE 16 report to meet their own compliance needs-potentially saving these organizations significant time and money on auditing fees.

By leveraging NaviSite's services through one of our SSAE 16 compliant locations, you can be assured that NaviSite has met strict standards in the following areas:

- **Physical Security:** Physical access to the data center and other sensitive areas is restricted to appropriately authorized personnel, protected by a combination of physical security presence and biometric identification
- **Logical Authentication and Access:** Logical access to networks, programs, and data is restricted to appropriately authorized personnel
- **Security Monitoring:** System vulnerabilities are identified; unauthorized attempts to gain access to systems residing on NaviSite networks are detected and addressed immediately
- **Systems implementation:** Implementations of system software/hardware and application software are appropriately authorized, tested, approved, and documented
- **Systems Enhancements and Maintenance:** Changes to system software and hardware, as well as application software, are appropriately authorized, tested, approved, and documented
- **Problem Management:** System related problems are identified and resolved in a timely manner
- **System Backup:** Critical production programs and data are backed up regularly to redundant systems
- **Environmental Controls:** Anti-static tiles, controlled temperature and humidity