

LightPort Security, Reliability, and Compliance Assurance Statement

LightPort is committed to maintaining the privacy and security of our Client's Web sites and confidential information. We have gone to great lengths to ensure the reliability and integrity of the LightPort infrastructure. Below is a brief overview of a few of those areas that we address to protect our clients as well as their clients:

Security

- **Encryption:** LightPort uses secure encrypted connections for display and transmittal of "sensitive" data. VeriSign™ (<http://www.verisign.com>) was chosen to provide Secure Server IDs for LightPort's customers because of their industry-wide reputation for quality and reliability. We use the highest grade of encryption allowable by the U.S. government to protect data transmissions (currently 128bit encryption, also known as Strong Encryption).
- **User IDs and Passwords:** LightPort creates every site with the capability of password-protecting information as deemed necessary by the site's owner. Every User ID and Password is completely configurable. Access is granted to individual pages in the site by "explicit authorization."
- **Portfolio Reporting Authentication:** Every folder or account in the Reporting System must have explicit permissions granted to it for access by Web site users. Each client portfolio is segregated on our servers from other portfolios. Report Data is transmitted using 128bit encryption.
- **Peer Review:** Numerous tier 1 prime brokers and broker dealers have selected LightPort to provide Internet services to their advisors and Investment Managers. LightPort also provides Web development and hosting services directly for those organizations in most cases.
- **Network Architecture:** LightPort has designed a hosting environment that adheres to the strictest of Internet security standards. We routinely monitor our firewalls, proxy servers, encrypted connections, and access policies to ensure the continued security of our systems. Databases that contain User Ids, Passwords, Permissions or other sensitive information are located on an internal network segment that is not directly accessible via the Internet. All Web servers are located behind at least one Firewall.
- **Vulnerability Assessments:** LightPort has successfully completed audits and/or vulnerability assessments of business processes, application integrity, and system/physical security by several industry-recognized information security firms. LightPort has regularly scheduled assessments performed by an industry recognized 3rd party.
- **Policies/Procedures:** LightPort's information security policies and procedures govern the following: passwords, non-disclosure of information, customer password access, distribution and equipment usage, employee termination, development lifecycle, release management,

site creation, site security settings, Web server creation, Web server security, back-up and recovery, disaster recovery and security breach.

- **Security Awareness:** Information security is a high priority at LightPort. Each LightPort employee is aware of the sensitive nature of the information that is housed in the data center. All new research and development that occurs must comply with the strictest information security standards to ensure the integrity of customer data. All Web servers and database servers are audited for both successful and failed events. Log files are configured with appropriate access control. Security logs are reviewed on a regular basis. Security logs are backed up and stored off site for seven years. Employees are required to keep a clean workplace free from any Customer data and to lock workstations when they are not in use.

Reliability

- **LightPort Data Center:** The data center is a fully redundant facility that is designed to ensure optimal, 24/7/365 performance of your mission critical applications. Direct Optical Co-location Connections (DOCC) with two of the nations leading Tier-1 providers, MCI (formerly UUNet) and Time Warner Telecommunications, eliminate trouble prone local loops. This connectivity model will provide the best end user experience by immediately facilitating content delivery to the providers' backbones. The network design, systems monitoring, and expert support staff will provide clients with a highly stable environment that provides 99.99% bandwidth, power and connectivity uptime.

The Data Center operates a Cisco Powered Network utilizing Virtual Local Area Network (VLAN) technology to segregate client traffic, which prevents data sniffing within the data center and mitigates the potential exposure & scope of denial of service attacks. Redundant fast Ethernet connections are provided to the LightPort Servers, providing high availability directly from the point of connectivity to LightPort's equipment.

The facility is powered by diverse, redundant connections to two major power grids. Enterprise-class UPS systems and on-site diesel generators will protect LightPort systems from a loss of commercial power.

Closed circuit digital cameras, security breach alarms and card-swipe access points are present at all entry and exit points for maximum security.

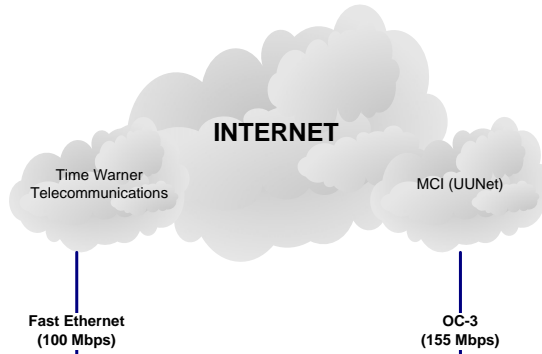
The Data Center also uses an Ansul Inergen fire suppression system to provide a waterless solution that is safe for equipment and personnel. This compliments the pre-action system consisting of ionization, heat, and photoelectric sensors that continually sample for the

presence of smoke or heat. A fully redundant environmental control system maintains a cool and humidity regulated environment to maximize the life of costly electronic equipment. Finally, 24/7 monitoring, alerting, and technical expertise surround all aspects of the data center to deliver the uptime and services that LightPort and our customers require.

- **Change Control:** All product development occurs in a separate development environment. All source code is maintained in Microsoft Visual Source Safe™. Product releases are first unit and system tested in the development environment. The release is then moved to a staging environment where integration testing is performed. The release is then packaged for installation into the production environment complete with rollback procedures. Releases are currently scheduled to occur on a bi-monthly basis during LightPort's scheduled maintenance windows.

Compliance

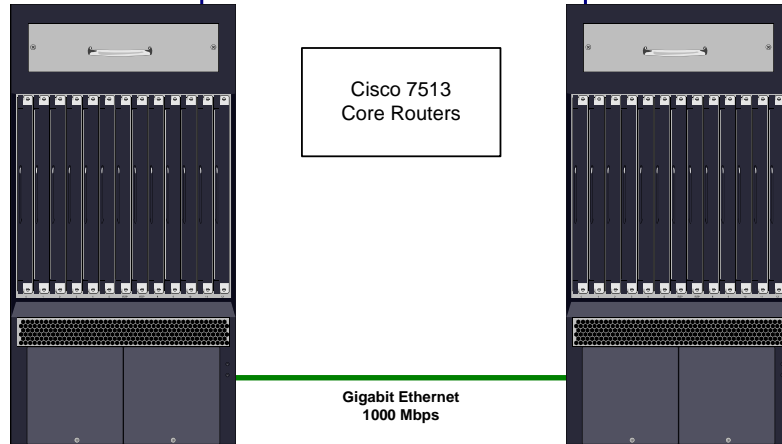
- **Privacy and Confidentiality:** In accordance to the Gramm-Leach-Bliley Customer Privacy Act the following is LightPort's privacy policy: LightPort does not disclose or use non-public personal information about your customers, and/or former customers, other than to carry out the purpose for which you disclosed the information, or as permitted by law. LightPort has adequate procedures to safeguard records and information of your customers, consistent with SEC Regulation S-P, and that information will not be disclosed to an unaffiliated third party for any reason, without your prior written consent.
- **Real-time Archiving and Back-ups of Web sites and Email:** LightPort provides two levels of archiving functionality. 1) Standard nightly back-ups for disaster recovery and off-site, long-term storage. 2) In addition to standard back-ups LightPort also archives Web site content as well as Email messages in "real-time." As such, the service captures every notice, recommendation, private message, portfolio report, statement, market commentary, public marketing presentation; in short, every element of communication that a firm posts to its Web site or sends via Email. LightPort is one of the few providers that can provide the advisor or manager a means to fully comply with current regulations, statutes, and rulings from the SEC, NASD and other governing organizations. The summary requirements of the regulations are these: 1) Copies of all regulated communications must be retained for 5 years; 2) Whatever means used must be organized, indexed, and be easily accessible.



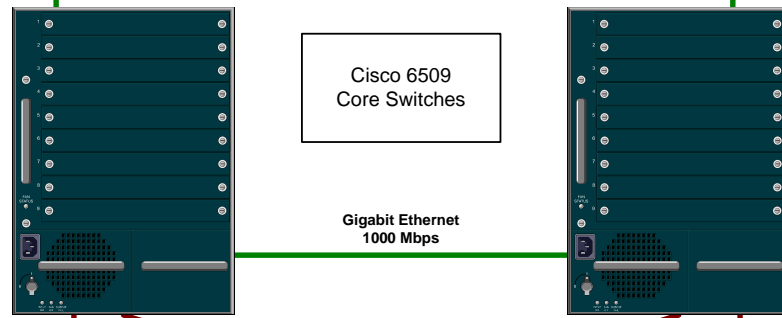
Fast Ethernet (100 Mbps)

OC-3 (155 Mbps)

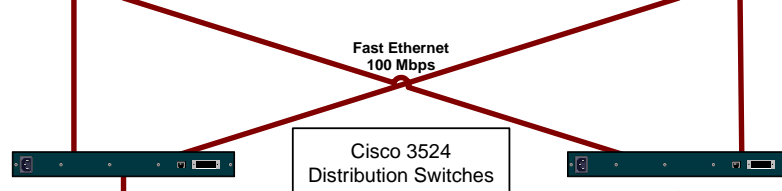
PEERING LAYER
The BGP4 protocol tracks available paths to destination networks and is essential to multi-homed environments



AGGREGATION LAYER
VLAN (Virtual Local Area Network) technology is used to isolate traffic and reduce the risk of being affected by denial of service attacks targeting other customers



DISTRIBUTION LAYER
HSRP (Cisco's Hot Standby Routing Protocol) is used to provide an alternate network path in the event of equipment failure



ACCESS LAYER
Multiple 100 Mbps or 1000 Mbps connections provide redundancy all the way to LightPort equipment

