

Nomadesk Security Statement

1 DATA CENTER SECURITY

1.1 SAS70 Type II Data center. (<http://www.sas70.us.com/>)

Nomadesk servers are all located in SAS70 Type II Certified Datacenters. Unlike Type I, the Type II examination requires that independent CPA auditors spend several days onsite to validate data center information technology processes, procedures and controls. SAS70 Type II audits provide customers with guarantees of security, reliability and operational effectiveness by service organizations such as data centers. The Sarbanes-Oxley Act identifies a SAS 70 Type II report as the only acceptable method for a third party to ensure a service organization's controls. In addition, SAS 70 is designated by the U.S. Securities and Exchange Commission (SEC) as an acceptable method to affirm a service organization's internal controls without conducting separate assessments. All data centers are strategically isolated from disaster/terrorism prone areas and offer unsurpassed connectivity, reliability and redundancy with 99.999% uptime. The Nomadesk server infrastructure HAS unprecedented global coverage, failover and geographic routing.

1.2 Data Center Credentials

- Security
 - 24/7/365 on-site security and technical staff
 - Multiple security cameras
 - Dual-Factor Biometric access controls and keypads
 - Double-locking mantraps at data center entrance
 - All cabinets, cages and suites are locking
 - Physical audit trails on all entry points
- Location
 - Unsurpassed connectivity, reliability and redundancy with 99.999% uptime guarantee
- Power Systems
 - Multiple city electrical grids
 - Redundant diesel generators
 - Redundant UPS systems by APC
- Environmental Controls
 - Internal and external n+1 cooling units
 - Constant ambient air temperature of 68° (+/- 5°)
 - Automatic humidity controls for 45% (+/- 5%)
 - Internal air cleaning & filtering systems
- Fire Suppression
 - Very Early Smoke Detection Apparatus (VESDA)
 - Pre-action, dry-pipe sprinkler systems
 - Integrated smoke/heat detectors

2 DATA TRANSFER SECURITY

All communication with the Nomadesk servers is enforced over a 128 bit encrypted SSL connection. Access to your files via the Web Browser is over https, secured by the Independent Third Party Security Agent Thawte (www.thawte.com) and is password protected.

3 INTRUSION DETECTION AND PREVENTION

Traffic to our servers is constantly monitored by state of the art intrusion detection systems on both a hardware and software level. There are multiple levels of firewalls and there is a process defined for daily, weekly and monthly scheduled manual review of the security logs.

4 THIRD PARTY AUDITS AND REVIEWS

The entire Nomadesk infrastructure is tested and audited by an independent third party security expert organization, (<http://www.zionsecurity.com/>). They perform regular security checks and tests on the Nomadesk infrastructure. These tests include penetration tests and scans. Furthermore we have a formal monthly security board with independent security contractors. Based on the outcome of these boards, we apply patches and fixes and define the strategy for (further) development of our software with state of the art security measures in mind.

5 SECURITY ON YOUR COMPUTER

Your files are stored locally on your computer on a 256 bit AES encrypted file system. Nomadesk file servers can only be mounted and decrypted by using your personal password and unique identified. In case of loss or theft of your computer you can remotely shred the local data contained on the Nomadesk File servers. (Theftguard™)

6 APPLICATION SECURITY

Nomadesk server architecture and client software is designed in such a way that access to all servers goes through an authentication mechanism, followed by an access control verification that only permits access to approved file servers. At any time access can be revoked by the owner of the file server or by Nomadesk system engineers should there be a security incident.

7 HIPAA COMPLIANCE

Nomadesk is a Business Associate to its customers who are Covered Entities. When you use our service to store electronically Protected Health Information (PHI), we do confirm that our Physical and Technical Safeguards are compliant with the Security Rules as described by the Standard on Feb 20, 2003.

(http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act).

Administrative safeguards as defined by the security rule are the responsibility of the customer.