

White Paper on Security and Disaster Recovery

Security

MegaNet considers network and information security to be of the utmost importance in delivering storage applications and services to our customers. Network and information security are core differentiators of our offering. From our personnel to our technology and policies, security is built in to every aspect of our operations and solutions. We apply a 'Defense in Depth' security model, which addresses security from many different perspectives. These include:

- 1) Privacy Assurance and Administrative Security
- 2) Physical Security
- 3) Firewall, Access Control, Hacker-Cracker Defense
- 4) Strong Factor Authentication
- 5) Encryption

Privacy Assurance and Administrative Security - MegaNet actively restricts access to the physical site and machines where customer data is stored to only key members of the MegaNet staff who have a need-to-know. In other words, although we have many developers on staff, only a small portion of the team can physically access our ASP server farm. Our systems are secured in a multi-layer fashion that grants rights (from physical to virtual access) to a subset of personnel.

Physical Security - MegaNet provides physical security at a level that most businesses will recognize as better than that which can be provided by them. MegaNet's physical operations are serviced by four independent high-speed Internet connections, and have redundant power supplies that can run independent of the local power grid for more than 45 days. Access to our hosting site is restricted to those personnel who have been placed on an access control list by the MegaNet security manager - no one else can add a name to the access roster. Personnel onsite must present identification credentials and then successfully be authenticated through 2 biometric scanners before entrance to the interior portion of the structure is granted. At that point, security staff must escort personnel to the locked areas where MegaNet servers are located. Security staff logs each access event. Roving guards in conjunction with a sophisticated closed circuit television network actively monitor the entire facility.

Firewall and Access Control - MegaNet employs best practices in its firewall and access control systems. Defense is provided by our use of cutting-edge firewall technology and managed security services provided by a dedicated security monitoring team. MegaNet's network architecture assures that only limited Internet protocol (IP) addresses are exposed over the Internet. Although our network utilizes multiple servers on our back-end, only specific IP addresses allow users through our firewall. In other words, even though each machine has its own internal address, the world outside our perimeter can never access (or 'resolve') them. Attempts to maneuver around or through the firewall using unauthorized addresses are rejected, logged through an intrusion detection system, and investigated by the security team.

Strong Factor Authentication - All users of the MegaNet network must possess a current username/password/domain combination. Without all three data elements, a person will not be granted access to the MegaNet site. MegaNet does not permit anonymity, nor do we have a 'public folder' area. All users must be registered with MegaNet to utilize the service.