Database Services, Inc.
Security and Data Protection for Hosted Data for our
Hosted SQL Server Users and Web Services Pack Users

This white paper is designed to provide information for our customers who allow us to host their company data on our SQL Servers, or use our Web Services Pack to provide information to their clients.

Physical Security and Redundancy

We host your data in a secure, purpose built, level 3 data facility (Atlantic.net)
http://www.atlantic.net/About-Us/World-Class-Data-Center-Facilities.html

It has redundant power conditioning through inverters, redundant air conditioning, redundant internet connections, a backup diesel generator, locked doors, 24/7 security, and waterless fire detection and suppression equipment. Access to this facility is limited to people pre-registered on an access list with a picture ID. Each server cabinet is individually locked.

We stage two identical SQL Servers at this facility for your data, one is primary and one is mirrored. The "data gap" between the two is measured in milliseconds. Each server has redundant power supplies and uses a RAID drive array. We make backups every half hour to a third hard drive.

As long as you are keeping the PST Web Services pack up and running, a fourth copy of your data is available on yet another server at Atlantic.Net and can be reconstructed and made available for you in a matter of hours.

Finally, in the very unlikely event that Atlantic.Net is taken completely out of service, your data is copied to another location several miles away on a continuous basis. We mirror the PST Web Services Pack server from Atlantic.Net through a secure Virtual Private Network (VPN) to another server in our corporate offices. That fifth copy of your data varies from a few milliseconds to a few hours out of date depending on the rate of updates.

Internet Security

While we can provide good physical security and backups for your data without your help, providing good electronic security requires effort from both you the customer and us as your provider.

Our SQL Servers sit behind a firewall at Atlantic.Net. Only requests for a specific IP address on a specific port are forwarded to the server hosting your data.

You connect to your hosted data or the PST WSP Server over the internet through the PST program. As you start PST, you have to provide your login and password combination to allow the program to connect to our servers. That login process takes place using 128 bit encryption. It is very unlikely that outsiders will find your credentials by “listening in” anywhere on the internet.

We require that passwords used to access your hosted data consist of at least 8 characters, and one of them must be non-alphanumeric. Strong passwords are one piece of a good defense against unauthorized access.

Now for the hard part: You have to keep your data access passwords private. If you use an easy password, write it on a Post-it note and stick it to your monitor, fail to change the password when an employee leaves your company, you are compromising your data!