Security Questions & Answers about TestWiz™

1. **What do you do to secure the test result information?**
   Several steps are taken to secure all the information stored in TestWiz:
   
   - The data is kept on a separate server away from the web interface and housed at a secure facility. The data itself is stored in the database in an obfuscated manner with anonymously named fields.
   - The system is protected by a high quality firewall, which in turn is managed externally.
   - Direct access to the servers is strictly limited to a small number of key employees. All employees have signed an agreement to honor privacy of data, and they do not access the site unless required to perform their jobs.
   - Customer passwords can be up to 50 characters long.
   - Customer passwords are not stored in our database. Instead, a salted cryptographic hashcode is stored. When a user enters his/her password, the salt and password are rehashed, and if that hash matches that which is stored in the database, the password is accepted as being valid.
   - Password guessing is prevented by automatic lockout after five failed login attempts in 5 minutes, after which the account is locked for 10 minutes.
   - Customers can request strong password requirements for users changing their own passwords. This is based on our own internal rating system for password strength. Currently, a password containing seven characters with mixed case letters and one digit is required by default. Each customer can have a stronger requirement if desired. It is very important that customers use strong passwords and keep them secret.

2. **Do you have off-site backups?**
   Yes, we have two independent backup systems. One system backs up to a separate drive system (directly attached storage or DAS). The other backup is to our off-site system provider’s backup system. Both are redundant to each other. The DAS system is for rapid restoration of customer specific data. The off-site backup has a two-week retention and a much longer/all or nothing restoration pattern. Our customer service team can restore your data to some prior version in a matter of minutes.

3. **How frequently do you back it up?**
   Rapid online backup/restoration: Daily full with a two week tail; Weekly full with a 4-6 month tail. Off server backup/restoration: Daily incrementals; Weekly fulls with a two week tail.

4. **Has anyone tried to hack into the TestWiz website?**
   The TestWiz firewall log shows continual attempts to probe TestWiz for security vulnerabilities. We are not aware of any successful “hack” into TestWiz. All access to TestWiz is logged. The logs are periodically reviewed for signs of breach.