



ASQ Online Technical Information

Technical details for system requirements, privacy policy, and security features of **ASQ Online, which includes ASQ Pro, ASQ Enterprise, ASQ Hub, and ASQ Family Access** (www.asqonline.com).

About ASQ Online

ASQ Online is an Internet-based application, hosted on Brookes Publishing Company's servers in Littleton, MA with a Tier-1 Managed Hosting Company.

ASQ Online is a Ruby Rails application, using a MySQL Server database.

ASQ Online Requirements

Each user computer must have the following:

- Any PC running Windows® 98, 2000, XP, or Vista or Macintosh® OS9 or higher, with one of the following browsers: Internet Explorer 6.0 or higher; Netscape 9.0 or higher; Mozilla Firefox; Safari
- Browser must be configured to accept cookies.
- Browser must have JavaScript enabled.
- To view demos and tutorials, the free Adobe Flash Player (<http://www.adobe.com/products/flashplayer/>) is required.
- To view and print reports, questionnaires, and other documents, the free Adobe Acrobat Reader® (<http://get.adobe.com/reader/>) is required.

Account Security

Security Overview

Brookes Publishing is committed to keeping your data safe, secure, and private. Our tier 1 hosting company, Fused Solutions LLC, has received its SAS 70 Type II certification, one of the most widely recognized auditing standards for service companies. Fused Solutions LLC reached this level of recognition for its reliability, security, and ability to safeguard IT operations. We protect your information with industry standard Internet security measures and have the appropriate physical and technical safeguards in place. When you use our secure online services, we protect your data in a secure, restricted-access environment. Your account information or specific assessment data remains yours and cannot be shared with any third party without your prior approval.

Network Security

Browser-level encryption protects all of your confidential data and information. ASQ Online uses 128-bit Secure Sockets Layer (SSL) encryption, which is also employed by most financial institutions, medical data centers, and government agencies to ensure that data is secure from interception during transmission. To authorize and certify access, we use VeriSign, an advanced security solution designed to provide secure communications and transactions over the Internet and private networks. SSL prevents unauthorized access to your data.

Access Security

Our servers are protected by industry standard firewall technology. Only authorized traffic and requests from legitimate sources are allowed through our firewalls to ensure the safety of both user's data and our server equipment.

Data Security

Your information is stored on RAID 5 storage systems, which use redundancy to protect against data loss and are designed to recover data quickly in the event of a hardware or disk failure. Brookes Publishing takes precautions to protect the confidentiality and security of the data collected and stored in the site's database by using industry-recognized security safeguards such as firewalls, coupled with carefully developed security procedures to protect your information from loss, misuse, or unauthorized alteration.

Regular backups of the site and all data are made; all data are backed up in full on a weekly basis, with incremental backups being made daily. Backed-up data are stored at a secure site for a period of 90 days.

Physical Security

Our databases and the servers on which we store site information are kept in a secure Tier 1 data center that includes physical security, conditioned power, environmental controls, uninterruptible power supplies, diesel generator, and fire suppression technologies.

Password Security

Users can only gain access to the system by providing a valid username and password combination, which is encrypted while in transmission. Password-protected information is only available to you or authorized users within your organization. No access is allowed to the site without a valid username and password combination. A username must be unique across the entire ASQ Online system, not just within a particular account. User passwords have a minimum length and are encrypted using a read-only method so they cannot be viewed or decrypted from the database.

Family Access Security

If you subscribe to Family Access, you can assure parents who enter data online, that we employ the same security and data protection protocols, mentioned in this document. These protocols will ensure 1) their data is secure from interception during transmission and 2) the prevention of unauthorized access to their data. Any data that is submitted by a caregiver can only be viewed by users who have authorized access to your account.