NJM Insurance Group

NJM Security Policy

Protecting Your Information:

NJM protects customers' information with physical, technical, and procedural controls and maintains compliance with federal and state regulations. We employ in-house as well as third party testing of our Internet accessible applications and IT systems to ensure your information remains secure. Our systems are monitored for unauthorized intrusion attempts and attacks.

NJM uses SSL (Secure Sockets Layer) protocol encryption to transmit private information on our Internet accessible applications. SSL encryption creates a secure connection between your browser and NJM's applications. You can identify when a webpage is secure by looking at the address of the webpage in the URL. The address will start with https: rather than http: and in most cases the browser will display a locked padlock icon when the page is secure.

For security reasons, we don't recommend you use a public computer or public Wi-Fi network connection. If you must use a public computer when accessing our Internet applications, NJM recommends that you clear the browser history and close the browser to remove any potential of your personal information being accessed after you leave the public computer.

Also note that our applications have been verified with Microsoft Internet Explorer 9+, Google Chrome 34+, Safari 5+ and Firefox 26+. The general user experience is best appreciated using one of these browsers.

What you can do to be more secure and help protect your information:

- Use your own workstation PC or tablet. Avoid using public/shared computers or public Wi-Fi networks.
- You should always use the latest available software and operating system versions for your workstation and configure your system to install security patches on a regular basis.
- Ensure that your Internet browser uses strong 128-bit encryption.
- Use anti-virus software and configure the software to install new virus updates automatically.
- Use a network firewall to protect your Internet connection from external attacks.
- Create a strong password using a minimum of 8 alphanumeric characters.
- Change your password regularly.
- Never share your accounts or passwords.
- Use a unique Username/Password for each web based user account.
- Be sure to always logoff the website and close your browser when finished.
- As an additional measure, you can also clear your browser's cache and temporary Internet files.
- Be suspicious and learn to detect phishing and malicious types of emails. Don't click on links within emails unless you're certain the email is safe. Don't respond to emails asking you to confirm your personal or private information. NJM will never ask you for this type of information via an email or email link.