NJM Security and Browser Policy

Updated July 2021

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 ourInternet accessible applications and IT systems to ensure your information remains secure. Our systems are monitored for unauthorized intrusion attempts and attacks.

NJM uses TLS (Transport Layer Security) version 1.2 protocol encryption to transmit private information on our Internet accessible applications. TLS encryption creates a secure connection between yourbrowser and NJM's applications. You can identify when a webpage is secure by looking at the address ofthe webpage in the URL. A secure webpage 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, you should avoid using a public computer or public Wi-Fi network connection whenaccessing our Internet applications. If you must use a public computer when doing so, NJM recommendsthat you clear **all** browsing history data (i.e., history, cookies, cached files, etc.) and close the browser toremove any potential of your personal information being accessed after you leave the public computer.

Supported Browsers:

We support the browsers shown below. If you are not using one of these browsers (or browser versions), please download or upgrade to a new browser or supported version using the link in the Desktop Environments table below. For tablets and smart phones, visit the appropriate App Store to upgrade your browser app. To verify which browser version you are currently using, please visit www.whatismybrowser.com.




If you choose not to upgrade your browser, your experience may not be optimal, or you may not be ableto use certain applications and tools on our website. In addition, you must enable JavaScript and browser Cookie support. We do not support beta and developer versions of any browsers or any browser extensions. If you are using a supported version of Internet Explorer, turn off CompatibilityView mode.

For optimal experience, we recommend using high speed internet over broadband connection.

Desktop Environments:

Desktop Browser	Windows 7 or higher	Mac OS X 10.10 (Yosemite) or higher	Latest Version Download
Google Chrome	Current and prior major release	Current and prior major release	https://www.google.com/chrome/browser/desktop/index.html
Apple Safari	Not Applicable	Version 9+	https://support.apple.com/downloads/safari
Microsoft	Edge	Current and prior major release	https://www.microsoft.com/en-us/edge
Mozilla Firefox	Version 51+	Version 51+	http://www.mozilla.org/en-US/firefox/

Mobile/Tablet Environments:

Mobile/Tablet	iOS (iPhone and iPad)	Android (phones and tablets)
Operating System	10.0 or higher	Current and prior major release
Browser	Safari	Chrome - current and prior major release

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

- Use your own device (PC, tablet, or phone). Avoid using public/shared computers and/or publicWi-Fi networks.
- You should always use the latest available software and operating system versions for yourdevice and configure your system to install security patches on a regular basis.
- Ensure that your Internet browser supports the TLS version 1.2 encryption protocol. Note thatall browsers in the above table support TLS version 1.2.
- 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. Do not click on links within emails unless you are certain the email is safe. Do not 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.