# SECURITY POLICY

Protecting our clients' personal information is of vital importance to M2 Trust Services LLC. All information submitted and transactions completed through this Website are confidential and secure.

M2 TRUST SERVICES LLC SECURE COMMUNICATIONS POLICY

Our system is designed so that data is encrypted as it travels to and from your PC. Every activity that you perform while logged in to M2 Trust Services' portal is encrypted using 128-bit encryption. This encryption is accomplished through Secure Sockets Layer (SSL) that is the Internet's defacto standards for data encryption. SSL allows users to establish connections with other secure Internet sites.

Secure Login
For security, an ID and password must be entered to access the website and your account. Additionally, the password you enter displays as asterisks so that no one else can see it. An account lockout condition has been set to prevent unauthorized access. After three consecutive failed attempts to access your account, access will be restricted and you will have to contact us. M2 Trust Services' staff does not know your password and do not need to know your password. No one from M2 Trust Services will ever ask you for your password.

Secure Environment (?)
To provide additional safety, M2 Trust Services' account access does not connect directly to the Internet. It is protected by firewalls – software and hardware products that are intended to define, control, and limit the access that outside individuals have to account access. As a general rule, firewalls allow only authenticated users to send or receive transactions through the system.

Automated Time Out
To help prevent unauthorized access to your account, your session on the website will automatically end after 15 minutes of activity.

Use of Cookies
We use "cookies" to help personalize your online experience. A cookie is a text file that is placed on your hard disk by a Web server. Cookies are not used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you, and can only be read by a Web server in the domain that issued the cookie to you. The use of cookies is a widespread industry standard and thus many major Websites use cookies. Cookies are primarily used to facilitate navigation of websites and as a convenience feature in the entering of information on websites.

You have the ability to accept or decline cookies. Most Web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience some features of M2 Trust Services' website.

Social Media Features

Our websites include Social Media Features, such as the Facebook Like button and Widgets, such as the Share This button or interactive mini-programs that run on our sites. These features may collect your IP address, which page you are visiting on our sites, and may set a cookie to enable the feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on our Websites. This Policy does not apply to features hosted by third parties. Your interactions with these features are governed by the privacy policy and other policies of the companies providing them.

What you can do to maintain security.

- Do not share your login credentials with anyone. If you lose your login Information, contact M2 Trust Services LLC immediately.
- Keep your user name and password secure.
- M2 Trust Services' client services representatives will NEVER ASK for your password when you call us for account assistance.
- Consider changing your password on a regular basis.
- Create strong passwords that do not include any personal information or common phrases.
- Be aware of your surroundings when logging in to your account. Make sure no one else is watching you when you type in your user name and password.
- To verify that your session is secure, look for an address starting with https:// instead of http:// and a secure symbol (closed padlock) on the status bar of your browser located on the lower part of your screen.
- Always log out if you must leave your computer for any reason and always remember to log off when you are done viewing your account.
- Promptly report unauthorized account access as soon as you are aware of unauthorized access.
- Always review all your confirmations and account statements to verify the accuracy of all account information and activity. Contact us immediately when you detect any errors, omissions, or inaccuracies.

Guidelines for Creating a Strong Secure Password

- The password must be between 8-20 characters and must include at least one letter, number and symbol (e.g. afhtfsf2$).
- Use a combination of uppercase and lowercase characters as well as numbers in your passwords.
- Do not use your name, your spouse's name, your pet's name, birthday, favorite food, or any personal information that others can easily obtain.
- Do not use a password that contains part of your user name or e-mail address.