

MAMRAMIM Security Policy

MAMRAMIM Loan & Note Marketplace is a trusted confidential application platform dedicated to providing secure online user access to its members.

MAMRAMIM employs a high degree of security consciousness. One of MAMRAMIM's priorities is to make reasonable efforts to ensure data security. Access, integrity, availability, ownership, authorization, dependability, authentication, and confidentiality are all major considerations within the MAMRAMIM platform Security Policy. Unfortunately, the Internet cannot be guaranteed to be 100% secure, and we cannot ensure or warrant the security of any information you provide to us.

MAMRAMIM upholds its stringent Security Policy with the following security measures:

1. Role-Based Usage

MAMRAMIM grants varying degrees of access to its users with different levels of authority within a provider practice.

2. Encryption

All communication between you and the MAMRAMIM server is secured using SSL AES 256-bit encryption. This is the highest level of encryption currently available commercially.

3. Data Security

MAMRAMIM takes measures to secure your data on its servers, and data center. Our data center is both physically and electronically secured. Our servers are isolated from the Internet by using a firewall which is a hardware and software system that blocks access by unauthorized parties.

4. Confidentiality

MAMRAMIM has internal policies that keep your data private and confidential. We will not share your data with any third party except as described in our Privacy Policy. Your data is your data only.

5. DDOS Protection

DDoS (Distributed Denial of Service) attacks are a type of cyber attack where an attacker floods a website or network with traffic from multiple sources, overwhelming the system's ability to function properly.

MAMRAMIM Offers Unmetered DDOS (Distributed Denial Of Service) Protection. DDOS protection is crucial because it helps to prevent or mitigate the effects of such attacks by detecting and blocking malicious traffic before it reaches the targeted system.

6. Login ID and Password

Access to your account is controlled by a login ID and a password, which you choose. Strict login ID and password rules help prevent unauthorized users from gaining access to data. We do NOT store a plain text version of your password. Your password is stored using a one-way hash key and verified using the same one-way hash every time you log in, which means no one at MAMRAMIM knows what password you have chosen. If you ever forget your password, we force you to choose a new one using an email verification check.

7. Auto Log Out

MAMRAMIM protects you against accidentally leaving your account active on a computer browser screen. The MAMRAMIM service ends your “session” if you are logged into MAMRAMIM but have not actively used the service for a set period of time. This prevents others from accessing your account when you leave a session and forget to log out.

8. 2 Factor Authentication

Two-factor authentication (2FA) is an additional layer of security that requires users to provide two forms of identification before gaining access to an account or system. It adds an extra layer of security on top of a username and password combination, making it much more difficult for attackers to gain unauthorized access.

2FA is important because passwords can be easily compromised through various means such as phishing, social engineering, or brute force attacks. 2FA, on the other hand, requires a second factor such as a token, mobile device, or biometric authentication, making it significantly more difficult for attackers to gain access to an account.

By implementing 2FA, organizations can significantly reduce the risk of unauthorized access, data breaches, and other security incidents. It also provides a higher level of trust and assurance to customers or users, increasing their confidence in the security of the organization.

9. Digital Certificates

Digital certificates are used to establish the authenticity and trustworthiness of a website and to ensure that communications between the website and users are secure. When a user visits a website that has a digital certificate, their web browser checks the certificate to verify that the website is legitimate and that the connection is encrypted.

The importance of using digital certificates on a website can be summarized as follows:

1. Establishing trust: Digital certificates are issued by trusted third-party certificate authorities, which verify the identity of the website owner. This helps to establish trust between the website and its users, which is essential for e-commerce websites, online banking, and other sites that handle sensitive information.
2. Protecting sensitive data: Digital certificates enable encryption of data transmitted between the website and its users, making it difficult for attackers to intercept and steal sensitive information such as login credentials, credit card numbers, and personal information.

Overall, using digital certificates on a website is essential for establishing trust, protecting sensitive data, and meeting compliance requirements. It provides users with the confidence to transact and communicate securely online and helps organizations to safeguard their reputations and avoid costly data breaches.

MAMRAMIM uses a digital certificate issued by ssls.com, a leading Secure Server Certification Authority. This gives you the confidence that you are connected to a site or application operated by MAMRAMIM and are authenticated as such.

10. Sensitive Information

MAMRAMIM handles all your information with respect to its confidentiality and privacy. We ask that you also follow your internet provider's policy on communicating sensitive information to and from your local computers to our servers.

11. Data Integrity

MAMRAMIM employs products and technology to help ensure data is available and access to the site continues without interruption.

12. Storage and Maintenance of Information

For more information regarding the storage and maintenance of information, please contact MAMRAMIM support.

13. Firewall

We take reasonable measures to secure your data on our servers and our data centers. Our data centers are both physically and electronically secured. Our servers are protected behind the Internet by using a firewall system that blocks access by unauthorized parties.

14. What can I do to protect my Privacy?

In order to protect your privacy while using MAMRAMIM, you can:

- a. Never share your sign-in name or password.
- b. Choose a strong password with upper and lowercase letters and numbers.
- c. Always sign out when you are finished using the service.
- d. Never share your two-factor Authentication code with anyone.
- e. Install and maintain anti-virus software and a firewall on all computers you use to access the MAMRAMIM service.
- f. Promptly install all security and software updates for your web browser and computer operating systems.