AAVAULT SECURITY POLICY

Effective date: **August 1, 2024**

1. **Introduction**

AAVAULT places high priority on the security of our platform and the protection of our users' data.

This Security Policy describes the measures we take to prevent unauthorized access, attacks and other security threats.

2. **Security measures**

We take the following measures to ensure the security of our platform and the protection of user data:
— Data encryption: All sensitive data transmitted and stored on our platform is protected by modern encryption methods.
— Monitoring and audit: Regular monitoring and auditing of our infrastructure for vulnerabilities and unusual activities.
— Update and patching: Timely updating and patching of software to eliminate known vulnerabilities.
— Backup and Restore: Regular backup of data to ensure its recovery in case of loss or damage.
— Employee training: Conducting regular cybersecurity training for our employees.

3. **User Responsibility**

Users are also responsible for the security of their accounts and data. We recommend that users:
— Use complex and unique passwords.
— Do not share your private data with other persons.
— Update your software regularly and use antivirus solutions.
— Be careful when dealing with suspicious emails and links.

4. **Security Breach Notification**

If we discover a security breach that may impact user privacy, we will notify users immediately and take appropriate action to address the threat.

5. **Changes to the Security Policy**

AAVAULT reserves the right to make changes to this Security Policy at any time. Changes take effect from the moment they are published on our platform.

6. **Contact information**

If you have any questions regarding this Security Policy, please contact us at: **mail@aavault.io**