

# Franklin Madison Responsible Security Disclosure Statement

Franklin Madison is committed to maintaining the highest standards of security across its systems and applications. If you discover or suspect a potential security vulnerability in any of our platforms, we encourage you to report it promptly through our Responsible Disclosure Program.

## Responsible Disclosure Reporting Process

Timely identification and resolution of security vulnerabilities are essential to protecting our users and infrastructure. If you identify a vulnerability in any Franklin Madison system, please report it immediately to our Security Team.

**Reporting Instructions:** Please include the following details in your report:

- Your contact email address
- A clear description of the vulnerability
- Specific location(s) where the vulnerability occurs
- Steps to reproduce or validate the issue
- Suggested remediation or fix
- Estimated impact of the vulnerability

Send your report to: [security@Franklin-Madison.com](mailto:security@Franklin-Madison.com)

## Responsible Disclosure Guidelines

- Franklin Madison does not offer monetary compensation for vulnerability reports under this program.
- Anonymous reports are accepted, but Franklin Madison may not engage further with unidentified reporters.
- We expect all participants to act in good faith and comply with these guidelines.
- Reports that are vague, unverifiable, or submitted in bulk without quality may be disregarded.

## Acknowledgment

The Franklin Madison Security Team will acknowledge receipt of qualified vulnerability reports via email. We appreciate your efforts in helping us maintain a secure environment.

## Disclaimer

Franklin Madison Responsible Disclosure program may change at any time without notice. Issues are reviewed individually, and responses are not guaranteed. Use of this content is at your own risk. Franklin Madison reserves the right to update or modify this information at its sole discretion.