Privacy Policy

LAST UPDATED: NOVEMBER 2026

Marquette Associates, Incorporated ("Marquette," "we," and "our") is committed to protecting your privacy and personal information. This Policy describes how and why we collect your information.

We consider our client relationships our most important asset. We strive to maintain your trust and confidence in our firm, an essential aspect of which is our commitment to protect your account information to the best of our ability. We believe that all of our clients value their privacy, so we will not disclose your account information to anyone unless it is required by law, at your direction or is necessary to provide you with our services. We have not and will not sell your account information to anyone.

Marquette collects and maintains your account information so that we can provide investment consulting services to you. The types and categories of information we collect and maintain about your organization include:

- Information we receive from you to provide investment advice to you (such as your address, telephone number, tax identification numbers and bank account numbers)
- Information that we generate to service your account (such as Asset Allocation Studies, Investment Policies and Executive Summaries)
- Information that we may receive from third parties with respect to your account(s) (such as custodial or brokerage statements and actuarial reports)

To provide you with the highest level of investment consulting services, we may disclose your account information in limited circumstances, which include:

- Disclosures to financial service companies as permitted by law, including those necessary to service your account (such as providing account information to investment managers and custodians)
- Disclosures to non-financial service companies that perform services on our behalf (such as our technology consultants who assist us in maintaining our computer systems)
- Arrangements with companies not affiliated with Marquette Associates will be subject to confidentiality agreements.

We will not disclose any account information about our current or former clients or their account(s) unless we receive prior consent, we believe the recipient is your authorized representative, or we are permitted by law to disclose information to the recipient.

Marquette will internally safeguard your non-public account information by restricting access to only those employees who provide products or services to you or those who need access to your information to service your account. In addition, we will maintain safeguards that meet federal and/or state standards to guard your non-public account information.

Our privacy notice is available for download on our website here.

Marquette maintains a comprehensive Incident Response Plan that outlines the procedures to be followed in the event of a significant cybersecurity incident. If unauthorized access to, or use of, customer records or information occurs, Marquette will promptly implement the Plan to facilitate timely detection, containment, mitigation, and remediation of the incident.

Marquette's Incident Response Team is responsible for coordinating response efforts and will notify appropriate clients, regulators, law enforcement authorities, and other relevant third parties as required by applicable law or when otherwise deemed necessary.

In addition, Marquette conducts ongoing oversight of its service providers through its Vendor Management Program, including periodic reviews and testing designed to assess compliance with Marquette's information security requirements and applicable regulatory obligation, including Regulation S-P.