

**PRIVACY POLICY DISCLOSURE**

*Thank you for your decision to invest with Northeast Private Wealth Management, Inc., DBA Platform Technology partners (“PTP”). PTP respects your privacy and only collects the information we need to service your account and administer our business. We are committed to keeping your information confidential and we place strict limits and controls on the use and sharing of your information.*

<p><b>What does PTP do with your personal information?</b></p>	<p>As a registered adviser, PTP must comply with SEC Regulation S-P, which requires registered advisers to adopt policies and procedures to protect the nonpublic personal information of natural person consumers and customers and to disclose to such persons, policies and procedures for protecting that information.</p>
<p><b>What information is protected by this policy?</b></p>	<p>PTP protects nonpublic personal information that we collect about current, prospective, and former clients, customers, and consumers. This includes any record containing nonpublic personal information that is maintained by or on behalf of PTP, including information received from you, from our affiliates or service providers, or from other financial institutions in connection with providing advisory services or administering our business.</p>
<p><b>What types of information does PTP collect?</b></p>	<p>The types of nonpublic personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> <li>• Information we receive from you through applications or other forms, correspondence, or conversations, including, but not limited to, your name, address, phone number, social security number, assets, income and date of birth</li> <li>• Information about your transactions with us, our affiliates, or others, including, but not limited to, your account number and balance, payment history, parties to transactions, cost basis information, and other financial information.</li> <li>• Information maintained in records or systems used to provide advisory services, service your account, meet legal and regulatory obligations, or administer PTP’s business.</li> </ul>

**How does PTP protect your information?**

To fulfill our privacy commitment we have instituted firm-wide practices to safeguard your personal information:

- We maintain physical, electronic, and procedural safeguards designed to protect your nonpublic personal information, including measures to detect, respond to, and recover from potential security incidents.
- We maintain physical, electronic, and procedural safeguards to protect your nonpublic personal information, to ensure that we are complying with our own policy, industry practices, and federal regulations.
- We restrict access to nonpublic personal information about you to authorized employees who need the information to administer your business.
- We do not disclose nonpublic personal information about our current or former clients to nonaffiliated third parties, except in the following circumstances:
  - As necessary to provide the service that the client has requested or authorized, or to maintain and service the client's account
  - As required by regulatory authorities or law enforcement officials
  - To the extent reasonably necessary to prevent fraud and unauthorized transactions.
  - Upon consent from the client.
- We may share information with service providers and vendors that assist us in servicing your account or operating our business. We require these third parties to maintain appropriate safeguards to protect your nonpublic personal information and to use such information only for authorized purposes.
- We do not participate in third party services that may collect personally identifiable information about your online activities over time or across different websites when using our website.
- We do not respond to browsers “do not track” signals or other mechanisms regarding the collection of personally identifiable information about your online activities over time or across different websites when using our website.
- Should your relationship end with PTP, your nonpublic personal information will remain protected in accordance with our privacy practices outlined in this policy.
- Annually, we provide a copy of our Privacy Policy Disclosure to clients.

**How does PTP respond to security incidents?**

PTP maintains a written information security and incident response program designed to protect the confidentiality and security of customer information. As part of this program, PTP has established procedures to detect, respond to, and recover from unauthorized access to or use of customer information.

These procedures include measures to:

- Identify and assess potential security events;
- Contain and mitigate unauthorized access to or use of customer information;
- Restore the security and integrity of affected systems and data;
- Evaluate whether sensitive customer information was or is reasonably likely to have been accessed or used without authorization; and
- Review and improve safeguards following a security incident.

<p><b>What happens if your information is involved in a security incident?</b></p>	<p>If PTP determines that your sensitive customer information has been accessed or used without authorization or is reasonably likely to have been accessed or used without authorization, PTP will provide clear and conspicuous notice as required by applicable law. Notice will be provided as soon as practicable, and not later than 30 days after PTP becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, unless a longer period is permitted by applicable law or requested by law enforcement.</p> <p>A notice will include, to the extent known and as applicable:</p> <ul style="list-style-type: none"> <li>• A description of the incident;</li> <li>• The type of sensitive customer information involved;</li> <li>• Steps you can take to protect yourself from potential harm;</li> <li>• Contact information for PTP; and</li> <li>• Information regarding additional resources that may help you protect your information.</li> </ul> <p>PTP may determine that notice is not required if, after a reasonable investigation of the facts and circumstances, PTP determines that the sensitive customer information has not been and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience.</p>
<p><b>How does PTP oversee service providers?</b></p>	<p>PTP maintains policies and procedures reasonably designed to oversee service providers that maintain, process, or otherwise have access to customer information on PTP's behalf. These procedures are designed to require appropriate due diligence and monitoring so that service providers take reasonable measures to protect against unauthorized access to or use of customer information and notify PTP of security incidents involving customer information systems maintained by the service provider.</p>
<p><b>How does PTP retain and dispose of your information?</b></p>	<p>PTP retains personal information only for as long as necessary to fulfill business and regulatory requirements. When information is no longer required, PTP disposes of it in a secure manner designed to prevent unauthorized access or use.</p>
<p><b>How does PTP document its information security practices?</b></p>	<p>PTP maintains records of its information security program, incident response activities, customer notifications, service provider oversight, and related compliance efforts in accordance with applicable regulatory requirements.</p>