HAMPTONROCK

WEALTH

# HamptonRock Wealth Management Privacy Policy

HamptonRock Wealth Management complies with all relevant regulations, including Regulation S-ID, Regulation S-P, and the Gramm-Leach-Bliley Act, which require us to establish policies to protect "nonpublic personal information" (NPI) and disclose these policies to our clients.

**What Information We Collect**

We collect NPI, which includes "personally identifiable financial information" such as your financial accounts, personal details, services you receive from us, and any analyses based on this information. This also applies to any lists or descriptions of customers derived from this information. For further details on protecting your information from cyber threats, refer to the "Cybersecurity Policy" section.

**How We Protect Your Information**

We employ a variety of measures to safeguard your personal information. These measures include:

- **Employee Training**: New and existing employees are required to review and acknowledge our privacy policies and compliance manual.
- **Limited Access**: We restrict access to your information. Employees are prohibited from sharing personal client information over the phone or via email unless they verify the recipient is you or your authorized representative.
- **Secure Records**: Physical client records are stored in locked file cabinets or rooms, and our office is secured outside business hours.
- **Digital Safeguards**: We use strong passwords, firewalls, and other appropriate security measures to protect electronic data. We destroy sensitive paper documents using shredders or other secure methods.

**Privacy Notices**

We provide all clients with an initial privacy policy notice when the relationship is established, and again annually. We maintain documented proof of these deliveries.

**Identity Theft Prevention Policy (Regulation S-ID)**

We follow an Identity Theft Prevention Program (ITPP) that includes the following components:

1. **Identification of Red Flags**: We monitor indicators of identity theft, such as fraud alerts on consumer reports, discrepancies in identification documents, or inconsistent personal details. We also respond to reports from clients or law enforcement about fraudulent activity.
2. **Detection Methods**: Our staff is trained to carefully verify identification, check customer names against regulatory lists (such as OFAC), and ensure all applications are reviewed for potential fraud.
3. **Responding to Red Flags**: When red flags are detected, we take appropriate action based on the risk level, such as requesting additional identification or halting the transaction if fraud is suspected. Suspicious activities may be reported to regulatory bodies.
4. **Program Updates**: Our ITPP is periodically reviewed and updated to address new risks and regulations.

## Cybersecurity Policy

Our cybersecurity policy is designed to protect both your personal information and our proprietary data. The security, integrity, and availability of the information stored or transmitted through our systems is a critical priority for us. We conduct regular vulnerability assessments to identify risks based on our technology use, third-party vendors, and potential cyber threats.

## Cybersecurity Procedures

1. **Periodic Risk Assessments**: We regularly analyze our information systems to evaluate risks to confidentiality, integrity, and availability. This includes assessing physical devices, software, and network connections. We implement measures to mitigate any identified vulnerabilities.
2. **Information Systems and Controls**: We protect our systems and information from misuse, theft, unauthorized access, and destruction using both physical and digital security measures:
    - **Software Ownership and Licensing**: All software used in our operations complies with licensing agreements, and we ensure timely updates and security patches.
    - **Virus Protection**: Anti-virus and anti-malware software are installed on all devices. Real-time scanning is always enabled, and updates are applied regularly to safeguard against new threats.
    - **Access Controls**: Access to client information is restricted. Employees must use unique IDs and strong passwords to access systems, and automatic timeouts are applied after periods of inactivity. Unauthorized access is prevented using encryption and secure pathways for remote access.
    - **Physical Security**: Physical access to information processing areas is restricted to authorized personnel. File servers with sensitive data are kept in secure areas.
3. **Data Transmission Security**: All data transmitted over communications networks, including wireless networks, is encrypted where feasible. Remote access to our network is only permitted using authorized devices and secure methods, such as VPNs.
4. **Mobile Device and External Media Security**: Storing client information on mobile devices or external media is prohibited unless explicitly approved. When approved, such devices must have password protection, auto log-off, and encryption. Mobile devices are not to be left unattended in unsecured areas.
5. **Equipment and Data Disposal**: When disposing of equipment or media, we ensure that private, confidential, or internal information is securely destroyed, either through verified on-site methods or trusted third-party vendors.

## Cyber Incident Response

In the event of a suspected or confirmed cyber incident, we follow strict protocols to contain the breach, assess its impact, and notify affected clients as required by law. Our team remains vigilant and regularly reviews cybersecurity trends to enhance our defenses.

## Ongoing Employee Responsibility

All employees are responsible for protecting client information and adhering to cybersecurity protocols. Any violation of these policies may result in disciplinary action, including restricted access or termination.