Cybersecurity Policy

Omnes Wealth Management LLC

Effective Date: January xx, 2026

CONFIDENTIAL – NOT TO BE DISTRIBUTED OUTSIDE THE FIRM

This Cybersecurity Policy is the property of Omnes Wealth Management LLC and its contents are confidential unless approved by the Chief Compliance Officer.

Using this Cybersecurity Policy

Each Supervised of Omnes Wealth Management LLC must read and understand the Cybersecurity Policy and comply with all of the policies and procedures herein.

Table of Contents

1. Cybersecurity Policy Objectives and Scope 3
2. Potential Cybersecurity Sources 3
3. Controls to Address Cybersecurity Sources 4
4. Access to and Viewing of PII, PCI and Internal Information 6
5. Responding to a Cybersecurity Attack 9
6. Testing the Cybersecurity Policy 10
7. Updating the Cybersecurity Policy 10
8. Definitions 10

1. Cybersecurity Policy Objectives and Scope

Objective
Omnes Wealth Management LLC ("Omnes Wealth" or the "Advisor") has adopted this Cybersecurity Policy ("Policy") to provide guidance to Omnes Wealth employees, contractors and those subject to Omnes Wealth's compliance program (collectively "Supervised Persons") for the storage or transmission of confidential digital information. It is the objective of this Policy to describe the safeguards and procedures for ensuring that information entrusted to Omnes Wealth by its clients is not acquired or transmitted by any unauthorized individual or entity. This Policy is also intended to address suspected privacy policy breaches pursuant to Regulation S-P in addition to identity theft red flags and how those red flags are addressed pursuant to Regulation S-ID.

Scope
This Policy applies to all Supervised Persons of Omnes Wealth and any digital storage device or medium that is under the control or ownership of Omnes Wealth or otherwise authorized to, or is intended to, store personal information about a client of Omnes Wealth.

Responsibility
Omnes Wealth has assigned the Advisor's Chief Compliance Officer ("CCO") as the individual with primary responsibility for implementing and revising this Policy ("Responsible Person"). The Responsible Person may delegate all or a portion of these responsibilities to a delegate of their choice, so long as that delegate is an employee of the Advisor or a third-party entity that is reasonably capable of implementing this Policy.

Enforcement
Any Supervised Person found to have violated the requirements of the Cybersecurity Policy may be subject to disciplinary action, up to and including termination of employment or contract, in addition to subsequent legal ramifications. Violators of local, state, federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution. Any questions about this policy should be directed to the Advisor's Chief Compliance Officer.

2. Potential Cybersecurity Sources

Internal
A source of potential Cybersecurity vulnerabilities is from the conduct of Supervised Persons of Omnes Wealth. Whether intentional or accidental, Personal Information about the client may be revealed or sent to someone outside the firm in a manner that exposes them to unreasonable Cybersecurity threats and potentially discloses the information to the public. Internal Cybersecurity sources may include but are not limited to:

- Sending sensitive data to wrong recipient – If you fail to review the recipients before sending Personal Information, the wrong recipient may receive Personal Information about a client unintentionally.
- Sending sensitive data through unsecured channels – If you transmit Personal Information without using approved secure communication methods, it may result in unauthorized access or exposure of client data.
- Sharing credentials for account access – If you share credentials with any other individual, the Advisor loses the ability to have an audit trail in their system access logs and the individual may further share the credentials or otherwise cause a Breach of Security.
- Account access not updated – If you access systems and information outside of your roles and responsibilities. Your access must be reviewed and adjusted to reflect your current role. Continuing to access systems or data that are not required of your role or outside of your function may create security risks and is not allowed.
- Securing the facility – If the Advisor's offices and devices are not secure when unoccupied, it can lead to a Breach of Security.

- Keeping systems updated – If the applications and anti-virus software is not kept up to date it can lead to security vulnerabilities that are more easily exploited and thus a Breach of Security.
- Use complex passwords – It is generally accepted that certain passwords are more vulnerable to others based upon the complexity of the characters used.
- Misplaced or stolen computers or devices – If computers or other devices are misplaced or stolen, it can lead to a Breach of Security.
- Inadequate disposal of physical or electronic records – Improper disposal of documents or devices can lead to exposure of sensitive data to third parties.

External
Cybersecurity vulnerabilities can also arise from external sources, such as messages received by Supervised Persons or Persons unrelated to the Advisor seeking to gain access to the Advisor's sensitive data for further attacks or violations. It is critical for any knowledge of external Cybersecurity vulnerabilities, or perceived breaches of the Advisor's network or information security controls to be escalated to the Responsible Person. External Cybersecurity sources may include but are not limited to:

- Clients – Clients may send files that have viruses in the normal course of providing requested information and therefore files and emails must be scanned for viruses.
- Vendors and Third-Parties – Similar to Clients, files and emails must be scanned for viruses.
- Suspicious Activity – Client email accounts may be accessed by an unauthorized individual or otherwise hacked, such that they attempt to transmit viruses to the account's contacts, upload malicious software, or seek to exploit the relationship with the Advisor by requesting funds.
- Phishing or Social Engineering Attacks – Malicious links and documents that are accessed or downloaded may result in unauthorized access to sensitive information.
- Identity Theft – A prospect, or someone acting as a client, may try to create an account with a false identity in order to gain physical access to the Advisor's office, or to create an expectation of receiving files that would be intentionally infected with a virus.
- Downloads – If computers are set to automatically download attachments there is a higher risk for cyberattacks.

3. Controls to Address Cybersecurity Sources

The Advisor has implemented the following controls to address the sources of Cybersecurity vulnerabilities as described in section 2 above. These controls seek to reasonably minimize any harm to the Advisor, its Supervised Persons and its clients, in response to a Cybersecurity threat or attack. The Advisor will ensure that Supervised Persons will only be allowed to access Information Systems and Sensitive Information for which they are authorized. User access privileges will be periodically reviewed to comply with this policy.

Internal
- Sending sensitive data to wrong recipient – Supervised Persons are expected to review the recipients before sending Personal Information.
- Email disclosures and footers – Supervised Persons that communicate using the Advisor's email domain will include a footer in their email signature that, should it be sent to an unintended recipient, be promptly deleted and not forwarded.
- Transmitting sensitive data – All files containing private client information must be transmitted using a secure, approved system or process. At no time should client Personal Information be sent over public networks in an unprotected format or shared on public websites or platforms.
- Storing sensitive data – All files containing client Personal Information in the Advisor's possession must be stored in a secure manner that restricts access to authorized individuals only. This includes storing data on password-protected devices or systems with

appropriate technical safeguards. At no time should private client data be stored on a device that is not protected by secure access controls.

- Credentials not shared – Supervised Persons are prohibited from sharing account credentials with any other person without the consent of the Responsible Person. Passwords must be kept private.
- Account credential review – The Responsible Person will review account credentials of systems used by Supervised Persons at least annually and update as needed to ensure access to the Advisor's systems by Supervised Persons is appropriate.
- Secure facility – The Advisor's offices will be locked when unoccupied.
- Misplaced or stolen computers or devices – computers and devices with the ability to access files containing Personal Information are password protected and the files are stored using encryption on the disk to ensure access only by authorized individuals. Supervised Persons are required to report any misplaced or stolen computers or devices to the Responsible Person, as described in Section 6 of this policy.
- Updating systems – The Responsible Person will review, at least annually, the status of applications, including anti-virus programs, to ensure that all available security updates are installed.
- Training – Cybersecurity training is ongoing. This Policy and any changes will be included in an at least annual compliance training agenda and Supervised Persons will be able to ask questions about the implementation of this Policy. Supervised Persons will complete a certification attesting to have participated in this training.
- Periodic risk assessments – An element of the Advisor's compliance program includes an annual assessment of its policies and procedures, including this Policy. The risk assessments will be kept with the Advisor's books and records for at least five (5) years from the date of completion.
- Data backup – The Advisor's critical data will be backed up as detailed in their Business Continuity Plan.
- Reporting concerns or violations – Supervised Persons are required to report any observed or suspected malicious activity from third parties or internal violations to the Responsible Person promptly and no later than end of the business day when it was first observed.
- Secure destruction – Any Personal Information will be securely destroyed to ensure that the Personal Information cannot be accessed by subsequent persons in possession of the disk or resource being destroyed by the Advisor.

External

- Scan for viruses – All files received, including email attachments or physical disks, from clients and vendors must be scanned for viruses.
- Remote access – All Personal Information of clients will be accessed remotely through an encrypted connection to the other computer before viewing or transmitting any personal information of clients. All personal information of clients is to be transmitted as described above under "Transmitting sensitive data".
- Updating systems – It is the responsibility to the Supervised Persons to ensure, both hardware and software applications, including anti-virus programs and firewalls, to ensure that all available security updates are installed when prompted. Supervised Persons are also responsible to notify the Responsible Person if any hardware and/or software is noticeably out of date, to ensure appropriate updates are installed.
- Suspicious activity – Supervised Persons are required to report any actual or potential suspicious activity observed to the Responsible Person promptly and no later than end of the business day when it was first observed. This includes any suspicion of identity theft involving clients or other Supervised Persons.
- Downloads – Turn off the option to automatically download attachments to minimize cyberattacks.

4. Access to and Viewing of PII, PCI and Internal Information

The Advisor recognizes the importance of verifying requests that involve the distribution of highly Sensitive Information or financial transactions. Identity presented through inbound emails or phone calls cannot be solely trusted. For any client-initiated request submitted via phone or email that involves updating contact information, modifying banking details, or executing a financial transfer to a previously unknown financial institution (e.g., a wire transfer with new instructions), the Advisor must perform a callback to a known representative of the client using a previously verified and trusted phone number.

Sensitive Information must be accessed and handled in accordance with the following standards:

- Minimize, to the extent possible, the use of personally identifiable information within reports, reviews, statements and other documentation.
- When material with Sensitive Information is sent, exercise due caution (e.g., registered mail, receipt confirmation, etc.) to assure that the material reaches its intended destination.
- When Sensitive Information is transmitted electronically, assure that such information is encrypted.
- Do not discuss Sensitive Information with or in the presence of unauthorized individuals.
- Secure completed applications and related materials to prevent unauthorized access.
- Sensitive Information must not be accessed out of curiosity, personal use, or without a legitimate business need.
- Verify the authenticity of recipients before disclosing Sensitive Information.
- Disclose Sensitive Information only to authorized parties, such as staff, other approved entities, or customers, and only when there is a legitimate business need.
- Only remove Sensitive Information from the Advisor's premises for legitimate business purposes. Use reasonable precautions, as well as the Advisor's procedures and rules, to ensure that the data remains secure and is not disclosed in an unauthorized fashion. Return such documents to the Advisor's premises as soon as possible.
- Customer account numbers must not be disclosed to unaffiliated third parties without written authorization from the customer.
- Sensitive Information received from unaffiliated financial institutions must not be disclosed unless permissible by applicable laws.

Onboarding
Before onboarding, all Supervised Persons with access to the Advisor's data and systems must undergo a pre-employment background check. Employment contracts and related terms should clearly define security roles and responsibilities. Account provisioning must be approved by the direct supervisor or the Responsible Person. The Advisor maintains an Onboarding Checklist to guide the onboarding process for new Supervised Persons. This checklist ensures proper access to systems, including hosted and cloud-based platforms, and confirms the provisioning of the Advisor's equipment, such as access cards and laptops.

Role Changes
If a Supervised Person's role changes, their access to systems and data must be reviewed to ensure it aligns with the responsibilities of the new role and maintains proper segregation of duties.

Terminations
In the event of a termination, access to all systems, including externally hosted platforms, must be promptly revoked. The Advisor utilizes an Employee Offboarding Checklist to ensure a comprehensive offboarding process when a Supervised Person departs. This checklist verifies that access to all systems (including hosted and cloud-based systems) is discontinued and that the Advisor's equipment is returned, including, but not limited to, access cards, mobile devices, and laptops.

Remote Work Security
The Advisor requires all Supervised Persons to adhere to the following security protocols:

- Secure Network Connections: Supervised Persons must connect to a secure, private network (e.g., home Wi-Fi or mobile hotspot). Public Wi-Fi must be avoided unless using a firm-approved Virtual Private Network (VPN).
    - Use secure virtual private network ("**VPN**") services when using public Wi-Fi provided at hotels, airports and other places where the network poses higher risk to computers. Do not let other systems use a device as an access point.
    - Use of a mobile phone hotspot is allowed so long as the hotspot is generated by a device under the control of Supervised Person, and which is otherwise compliant with the password requirements for third-party applications set forth in this WISP.
    - Supervised Persons sharing an office with a non-Advisor business must maintain a segregated network connection.

- Network Segmentation: Employees are encouraged to separate work and personal devices on different network segments where possible. Routers should have WPA3 or WPA2 encryption enabled, and default credentials must be changed.
- Endpoint Security: All firm-approved devices must have real-time endpoint protection, such as managed EDR (Endpoint Detection and Response) software. Employees must not disable or bypass security controls enforced on these devices.
- Screen Security & Privacy: Employees should use privacy screens in shared spaces and enable automatic screen lock after 15 minutes of inactivity to prevent unauthorized access.
- Lost/Stolen Devices: Any firm-issued device that is lost or stolen must be immediately reported to the Responsible Person for remote tracking, data wiping, and access revocation.

Securing Mobile Devices
Smart and/or Mobile Devices (e.g. smart phones and tablets) that are used to view, process, store or transmit any Advisor data, must have the following controls in place:

- All PII related to the Advisor should be segregated from any personal information stored on the same device. PII should only be accessed, stored or transmitted in or through applications that have been approved.
- Devices must require a password to access the device. Passwords must meet the minimum length required by the device.
- Biometric authentication methods (e.g., fingerprint) are permitted so long as associated device passwords meet or exceed the baseline requirements listed above.
- Failure to provide a correct password to a mobile device after no more than 10 attempts, or minimum attempts as required by the device manufacturer if greater than 10, must cause all data stored on the device to be permanently deleted.
- Devices must be set to auto-lock after no more than 5 minutes for smart phones, or 15 minutes for tablets, and require a password to regain access to the device.
- When a smart phone or tablet is left unattended, the user must lock the device.
- Any lost or stolen personal device that contains or has access to company data must be reported immediately to the Responsible Person.

Laptop and Desktop Computer Protection
The following policies are designed to protect the Advisor's laptops and desktops used for business purposes:

- Encryption
    - Laptops and desktops used for Advisor business must have whole disk encryption installed and active at all times.
- Firewalls
    - Laptops and desktops used for Advisor business must have a software firewall enabled. Built-in firewalls within operating systems satisfy this requirement when properly configured and activated.
- Anti-Malware Software

    - Laptops and desktops used for Advisor business must have anti-malware software installed. The software must be configured to automatically check for, download, and install updates.
    - The software must actively scan files in use and perform a full system scan on a regular basis.
    - Devices infected with malicious software must not be used until the infection is fully remediated.
- Patch Management
    - Operating systems must:
        - ➢ Be supported by their developers.
        - ➢ Automatically check for, download, and install security updates.
        - ➢ Be upgraded if they have reached "end-of-life" or "end-of-support." Devices with unsupported operating systems are prohibited.
    - Software applications must:
        - ➢ Be kept up to date with the latest security patches.
        - ➢ Be configured for automatic updates where possible.
        - ➢ Be manually updated promptly if automatic updates are unavailable.
    - If automatic updates are not feasible, a documented procedure must be in place to ensure timely patching of operating systems and software applications.
- Screen Lock
    - Devices used to view, process, store, or transmit Advisor data must lock the user interface after no more than 15 minutes of inactivity.
    - Supervised Persons must enter their password to regain access after the device locks.
    - When leaving a device unattended, Supervised Persons must manually lock the screen.

Electronic Device Travel Restrictions
To protect electronic devices (e.g., laptops, tablet PCs, portable media, cell phones/smartphones etc.) during travel:

- Do not store electronic devices in checked baggage.
- Do not leave electronic devices in plain sight in vehicles.
- Do not leave electronic devices unattended in a public place.

Physical Security
The Advisor uses physical security protections to maintain a safe workplace environment and to protect the Advisor's data and physical resources. These protections should include measures such as:

- Monitoring the building entrance by building security staff
- Auditable key card front-door access
- Privileged key access to the electronics equipment room
- The use of locked file cabinets, drawers, containers, or offices
- IT infrastructure should be stored within a secure room with access limited to Supervised Persons and vendors that require access for support, management, or oversight purposes.
- Require the check-in of visitors at reception and confirmation from a Supervised Person that a temporary access pass be granted. Short-term visitors should be accompanied throughout their visit.
- For hybrid or remote-first models, ensure secure storage of equipment and documents containing Sensitive Information. Home offices should use lockable filing cabinets and adhere to clean desk policies. Devices must remain encrypted and physically secured when unattended.

Acceptable Use
The primary purpose of the Advisor's information assets, including, but not limited to, computer systems, software, storage media, communication systems, and accounts providing email and internet access, is to support the ongoing operations of the Advisor. Reasonable personal use is permitted; however, under no circumstances are Supervised Persons authorized to engage in any activity deemed illegal under local, state, federal, or international law while using these assets. Supervised Persons are required to adhere to all practices outlined in this WISP. Following these practices is essential to safeguarding the Advisor from risks such as malware, system compromises, and service disruptions, as well as protecting the Advisor from potential legal liabilities.

Clean Desk
The Advisor recognizes that cleaning and building staff, among others, may retain access to the physical office space. Paper records containing Sensitive Information are to be stored in a locked office, locked cabinet, or other secure container that is on-premises. Additionally, they may be stored with outside counsel, or in a secure off-site facility, during non-business hours.

Data Governance
Supervised Persons must protect data according to its sensitivity as determined by the Advisor, based on business operational and financial risks, reputational risks, contractual obligations, and applicable legal and regulatory requirements. The Advisor has established three data classification levels, with examples outlined below.

- Public: Information whose disclosure would not have any negative impact on the Advisor, its clients, Supervised Persons, or business partners.
- Confidential: Unauthorized access to this information could impact the Advisor's operational effectiveness, result in financial loss, provide a competitive advantage to others, or negatively affect confidence. Typically, a breach involving confidential information would not necessitate client or regulatory notification or cause significant financial or reputational harm.
- Sensitive: Unauthorized access to this information could violate regulations such as Gramm–Leach–Bliley, Regulation S-P, and applicable privacy laws. It could cause significant damage to the Advisor's operations, reputation, or competitive position, result in substantial financial loss, or materially undermine confidence.

The Advisor has identified the following data sets and assigned them classification levels. Additional data sets may exist and should be classified accordingly:

Key Data Sets	Classification
Public regulatory filings (e.g., Form ADV)	Public
Published marketing materials	Public
Public website	Public
Incident Response Plan, Written Information Security Plan, and other Advisor policies and procedures	Confidential
General legal documents, service agreements, and contracts	Confidential
Human resources data, such as W-2s, W-4s, I-9s, background checks, salary and compensation information	Confidential
Vendor contact information: name, email address, and phone number	Confidential
Account statements and other investor documents that contain balances, account numbers, wire instructions, and SSN/EIN numbers	Sensitive

5. Responding to a Cybersecurity Attack

The response to a Cybersecurity attack will be reasonably related to the nature of the attack. Should a Supervised Person suspect their computer, device, or network has been subjected to a

Breach of Security, they will promptly notify the Responsible Person and provide any requested details to determine the nature of the Breach of Security and the extent of the Cybersecurity attack. The Responsible Person will document all related information, the results of analyzing such information, and any response to address the suspected or actual Breach of Security.

Appropriate responses may include, but are not limited to, monitoring client account(s), contacting the client, changing security settings, changing the Advisor's policies and procedures, closing the account(s), and/or notifying custodian(s) and law enforcement.

6. Testing the Cybersecurity Policy

Omnes Wealth shall review this Policy and test its effectiveness at least annually. The Responsible Person shall document the findings of the testing in a report to be kept with the Advisor's books and records.

Annually, Omnes Wealth shall also request or review available information from its Service Providers that store or handle client Personal Information to ensure they maintain a reasonably adequate Cybersecurity policy to support the activities of Omnes Wealth. Any deficiencies will be addressed with the Service Provider and documented in a report to be kept with the Advisor's books and records and/or the annual CCO report of the effectiveness of the Compliance Program.

7. Updating the Cybersecurity Policy

Omnes Wealth may make periodic updates to this Policy to account for changes in business practices, regulations and best practices. If any material changes are made to the Policy, all Omnes Wealth Supervised Persons shall receive a copy and be expected to certify their understanding of the plan.

8. Definitions

The following definitions are used within the regulation and are provided here for clarification:

Breach of security: the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a person. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Cybersecurity: the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

Electronic: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted: the transformation of data into a form in which meaning of the original data cannot be observed without the use of a confidential process or key to reverse the transformation.

Identity Theft: When a person assumes the identity of another in order to generate fraudulent transactions or other harmful conduct that impacts the assumed person to the benefit of the person initiating the transaction or conduct.

Owns or licenses: receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person: a natural person, corporation, association, partnership or other legal entity.

Personal information: a client's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such client: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a client's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record(s): any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider: any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

Suspicious Activity: activity that is indicative of fraudulent or illegal activity, or involves transactions that are not typical with a particular client, such as sudden requests to withdraw large sums.