Lyons Wealth Management, LLC
Procedures to Safeguard Client Records and Non-Public Personal Information
03/31/2026

LWM shall strive to: (a) ensure the security and confidentiality of consumer, customer and former customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of consumer, customer and former customer records and information; and (c) protect against unauthorized access to or use of consumer or customer records or information that could result in substantial harm or inconvenience to any customer. Accordingly, the following procedures will be followed:

A. Confidentiality. Employees shall maintain the confidentiality of information acquired in connection with their employment with LWM, with particular care taken regarding Non-Public Personal Information. Employees shall not disclose Non-Public Personal Information, except to persons who have a bona-fide business need to know the information in order to serve the business purposes of LWM and/or Clients. LWM does not disclose, and no Employee may disclose, any Non-Public Personal Information about a Client or former Client other than in accordance with these procedures.

B. Information Systems. LWM has established and maintains its information systems, including hardware, software and network components and design, in order to protect and preserve Non-Public Personal Information.

Passwords and Access. Employees use passwords for computer access, as well as for access to specific programs and files. Non-Public Personal Information shall be maintained, to the extent possible, in computer files that are protected by means of a password system secured against unauthorized access.

Access to specific LWM databases and files shall be given only to Employees who have a bona-fide business need to access such information. Passwords shall be kept confidential and shall not be shared except as necessary to achieve such business purpose. User identifications and passwords shall not be: stored on computers without access controls, written down, or stored in locations where unauthorized persons may discover them. Passwords shall be changed if there is reason to believe the password has been compromised. All access and permissions for terminated Employees shall be removed from the network system promptly upon notification of the termination.

To avoid unauthorized access, Employees shall close out programs and shut-down their computers when they leave the office for an extended period of time and overnight. Terminals shall be shut-down when not in use during the day and laptops shall be secured when leaving LWM premises. Confidentiality shall be maintained when accessing the LWM network remotely through the implementation of appropriate firewalls and encrypted transmissions.

System Failures. LWM will maintain appropriate programs and controls (which may include anti-virus protection and firewalls) to detect, prevent and respond to attacks, intrusions or other systems failures.

Electronic Mail. As a rule, Employees shall treat e-mail in the same manner as other written communications. However, Employees shall assume that e-mail sent from LWM computers is not secure and shall avoid sending e-mails that include Non-Public Personal Information to the extent practicable. E-mails that contain Non-Public Personal Information (whether sent within or outside LWM) shall have the smallest possible distribution in light of the nature of the request made.

Disposal. Electronic media, on which Non-Public Personal Information is stored, shall be formatted and restored to initial settings prior to any sale, donation, or transfer of such equipment.

C. Documents. Employees shall avoid placing documents containing Non-Public Personal Information in office areas where they could be read by unauthorized persons, such as in photocopying areas or conference rooms. Documents that are being printed, copied or faxed shall be attended to by appropriate Employees. Documents containing Non-Public Personal Information which are sent by mail, courier, messenger or fax, shall be handled with appropriate care. Employees may only remove documents containing Non-Public Personal Information from the premises for bona-fide work purposes. Any Non-Public Personal Information that is removed from the premises must be handled with appropriate care and returned to the premises as soon as practicable

D. Discussions. Employees shall avoid discussing Non-Public Personal Information with, or in the presence of, persons who have no need to know the information. Employees shall not discuss Non-Public Personal Information in public locations, such as elevators, hallways, public transportation or restaurants.

E. Access to Offices and Files. Access to offices, files or other areas where Non-Public Personal Information may be discussed or maintained is limited, and Employees shall enter such locations for valid business purposes only. Meetings with Clients shall take place in conference rooms or other locations where Non-Public Personal Information will not be generally available or audible to others. Visitors shall generally not be allowed in the office unattended.

F. Old Information. Non-Public Personal Information that is no longer required to be maintained shall be destroyed and disposed of in an appropriate manner. Refer to the Document Destruction procedures contained in the Maintenance of Books and Records policy for additional information.

G. Identity Theft. An identity thief can obtain a victim's personal information through a variety of methods. Therefore, Employees shall take the following actions to prevent identity theft:

a) When providing copies of information to others, Employees shall make sure that nonessential information is removed and that Non-Public Personal Information which is not relevant to the transaction is either removed or redacted.

b) The practice of dumpster diving provides access for a would-be thief to a victim's personal information. Therefore, when disposing of paper documents, paperwork containing Non-Public Personal Information shall be shredded, burned or otherwise destroyed.

c) To avoid a fraudulent address change, requests must be verified before they are implemented and confirmation notices of such address changes shall be sent to both the new address and the old address of record.

d) Employees may be deceived by pretext calling, whereby an "information broker" or "identity thief" posing as a Client, provides portions of the Client's Non-Public Personal Information (i.e., Social Security Number) in an attempt to convince an Employee to provide additional information over the phone, which can be used for fraudulent purposes. Employees shall make every reasonable precaution to confirm the identity of the Client on the phone before divulging Non-Public Personal Information.

e) LWM prohibits the display of Social Security Numbers on any documents that are generally available or widely disseminated (i.e., mailing lists, quarterly reports, etc.).

Employees could be responsible for identity theft through more direct means. Insider access to information could permit a dishonest Employee to sell Clients' Non-Public Personal Information or to use it for fraudulent purposes. Such action is cause for disciplinary action at LWM's discretion, up to and including termination of employment as well as referral to the appropriate civil and/or criminal legal authorities.

This notice is being provided to you in accordance with the Securities and Exchange Commission's rule regarding the privacy of consumer financial information ("Regulation SP"). Please take the time to read and understand the privacy policies and procedures that we have implemented to safeguard your non-public personal information.[1]

[1] Non-public personal information means personally identifiable financial information and any list, description or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available.

INFORMATION WE COLLECT

Lyons Wealth Management, LLC must collect certain personally identifiable financial information about its customers to provide financial services and products. The personally identifiable financial information that we gather during the normal course of doing business with you may include: 1. information we receive from you on applications or other forms; 2. information about your transactions with us, our affiliates, or others; 3. information we receive from a consumer reporting agency.

INFORMATION WE DISCLOSE

We do not disclose any non-public personal information about our customers or former customers to anyone, except as permitted or required by law, or as necessary to provide services to you. In accordance with Sections 248.13 through 248.15 of Regulation S-P, we may disclose all of the information we collect, as described above, to certain nonaffiliated third parties such as, but not limited to, attorneys, accountants, auditors and persons or entities that are assessing our compliance with industry standards. We enter into contractual agreements with all nonaffiliated third parties that prohibit such third parties from disclosing or using the information other than to carry out the purposes for which we disclose the information.

CONFIDENTIALITY AND SECURITY

We restrict access to non-public personal information about you to those employees who need to know that information to provide financial products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

280 W. Canton Ave STE 430, Winter Park, FL, 32789

Phone: (407) 951-8710

www.LyonsWealth.com