Tempo Wealth, LLC

POLICY AND PROCEDURES REGARDING INFORMATION SECURITY

Adopted Effective May 27, 2025

A. Introduction

[Tempo Wealth, LLC] ("Adviser" or "the Firm"), as part of conducting its business in the ordinary course, obtains and uses personal information of customers ("Personal Information") and employs proprietary resources and technologies, such as investment planning tools, trading strategies and formulas, and financial and economic analyses, to service those customers ("Proprietary Technology"). "Personal Information" generally includes the full name of a customer and one or more of the following categories of non-public information in the possession of Tempo Wealth, LLC: (i) the customer's Social Security number, (ii) the customer's driver's license number or state issued identification card number, (iii) the customer's bank, custodial, or brokerage account number combined with any security code, access code, personal identification number (PIN) or password needed to access such account. "Proprietary Technology" includes those systems developed or licensed by the Adviser, other than commercially available hardware and software, specifically designed to support Tempo Wealth, LLC's advisory business.

Personal Information and Proprietary Technology may be transmitted and retained in electronic and hardcopy form throughout the infrastructure maintained by Tempo Wealth, LLC, or may be licensed by or transmitted to Tempo Wealth, LLC from certain third-party vendors. Tempo Wealth, LLC acknowledges that it faces the risk of unauthorized access to and use of Personal Information and Proprietary Technology maintained by Tempo Wealth, LLC and third-party vendors (e.g., "cyber-attack"). The threat of such unauthorized access and use requires Tempo Wealth, LLC to identify and analyze the material risks to its business created by the use of such technology, and develop procedures for minimizing the risk, detecting unauthorized activity and remedying such unauthorized access and/or use.

As part of its assessment and analysis, Tempo Wealth, LLC has developed and implemented this information security policy (the "Policy"), taking into account the manner in which it operates its business, as well as any limitations on the scope of that business. The principal purposes of this Policy are:

1. Prevent unauthorized access and use of Personal Information and Proprietary Technology;

2. Detect and remedy unauthorized attempts to access Personal Information and Proprietary Technology; and

3. Eliminate substantial business interruptions due to cybersecurity threats.

This Policy complements Tempo Wealth, LLC's privacy policy and Business Continuity Plan (the "BCP"), particularly with respect to Tempo Wealth, LLC's obligation to safeguard Personal Information and recover operations from a cyber-attack or similar business disruption. The Policy also takes into consideration Tempo Wealth LLC's obligations (a) as an investment adviser registered with the SEC, and (b) if any, under the laws of the states in which its clients reside.

B. Governance

Tempo Wealth, LLC has designated ***the Chief Compliance Officer ("CCO") or Chief Technology Officer ("CTO")*** as the primary points of responsibility for coordinating the firm's efforts to develop and implement the Program. The ***CCO/CTO*** is Corbin Blackburn/ Timothy Farley.

The ***CCO/CTO*** will review no less than once per quarter to review the status of the controls and processes that Tempo Wealth, LLC has introduced to identify and mitigate cyber-risks, as well as any reports produced in response to periodic assessments of Tempo Wealth, LLC's cybersecurity program. The ***CCO/CTO*** will also assume responsibility for

1) Managing all hardware devices and software programs on Tempo Wealth, LLC's network so that only authorized devices are given access and only authorized software programs are installed and may execute on the network systems;

2) Training of all employees as to cybersecurity procedures;

3) Testing of cybersecurity procedures;

4) Maintaining a secured and confidential master list of all lock combinations, passwords, and keys and credentials; and

5) Evaluating the ability of third-party service providers to implement and maintain appropriate security measures for the Personal Information and Proprietary Technology to which Tempo Wealth, LLC has permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate security measures and indemnification for security breaches.

C. Cybersecurity Framework

The following Policy is premised on the framework proposed by the National Institute of Standards and Technology ("NIST") entitled Framework for Improving Critical Infrastructure Cybersecurity, as updated February 12, 2014 ("the NIST Framework"), *as amended*. The ***CCO/CTO*** will monitor updates and revisions to the NIST Framework and propose changes as necessary.

The NIST Framework recommends that organizations follow a structured program of cybersecurity that involves:

1) Inventorying the hardware, software and communications components of the organization's computer network and determining the risks to such components;

2) Describing their current and target states for controlling access to the computer network and data stored therein;

3) Detailing processes for monitoring systems to detect unauthorized access and attempts at unauthorized access to the network and stored data;

4) Planning for responses to unauthorized access and compromise of network resources and data; and

5) Recovering from cybersecurity breaches in a manner that restores operations and improves defenses against future cyber-attacks.

Both standards also include consistent review, monitoring and improvements to Tempo Wealth, LLC's cybersecurity procedures to integrate updated resources, technologies and risk awareness. Finally, integral to the cybersecurity procedures is the communication of this Policy to stakeholders, including employees, customers, vendors and third-party business partners.

D. Infrastructure Inventory Management

The ***CCO/CTO*** assumes responsibility for management (inventory, track, and correct) of all hardware devices and software programs on Tempo Wealth, LLC's network so that only authorized devices are given access and only authorized software programs are installed and may execute on the network systems. The ***CCO/CTO*** shall maintain an inventory of all hardware and software programs, which inventory will be updated as hardware and software is added or removed from the network.

The inventory of hardware shall include all devices connected to and/or used for accessing the Tempo Wealth, LLC network, including computers, printers, mobile devices, peripheral components, personal computers and tablets. (A copy of the hardware inventory shall be attached to this Policy as Attachment A.) The software inventory shall include all software installed on the Tempo Wealth, LLC network, including all software licensed from third-parties and proprietary programs executing on the network. (A copy of the software inventory shall be attached to this Policy as Attachment B.)

The ***CCO/CTO*** shall determine a schedule for monitoring and surveying the inventory of authorized hardware and software programs to ensure that the inventory remains current, and to detect and remove unauthorized hardware or software. We will be hiring an IT firm to continually monitor our software and cyber security systems. In addition, we will be using secure, encrypted programs such as Microsoft 365. Our programs we use will be dual factor authenticated, and we will have cybersecurity insurance as well.

Inventoried hardware and software will further be monitored by the ***CCO/CTO*** for security concerns, updates, maintenance and replacement, as necessary. Maintenance will be scheduled as necessary for hardware repairs and upgrades, and on no less than a SEMI-ANNUAL basis to download updates to authorized software programs. The ***CCO/CTO*** will monitor recommended

life cycles of hardware and software programs to avoid disruption to the Adviser's business operations due to infrastructure malfunction.

E. Risk Assessment

Before implementing the Policy, the ***CCO/CTO*** supervised the completion of a risk assessment (the "Risk Assessment"). The Risk Assessment is reasonably designed to identify foreseeable internal and external risks to the security, confidentiality, and integrity of Personal Information and Proprietary Technology, as well as the systems used by the Firm and critical third-parties to process such data. Such risks could result in the unauthorized disclosure, misuse, alteration, or destruction of that information or those systems.

Risks identified by the ***CCO/CTO*** include the following:

1. Unauthorized access through use of hardware connected to the network that is not properly configured with updated security software;

2. Unauthorized access and infiltration through authorized and unauthorized software programs, malware or other malicious code;

3. Unauthorized wireless access to the network, bypassing security perimeters by connecting wirelessly to access points;

4. Accidental or intentional disclosure of network user credentials to unauthorized parties;

5. Theft of customer, vendor, or authorized user identities and/or access credentials;

6. Unauthorized access through vendor or third-party security breach;

7. The alteration of systems data stored on compromised machines; and

8. Inability to recover data due to compromise of backup systems and databases.

The ***CCO/CTO*** will update these risks as necessary based on results of testing, lessons from the detection and responses to "Cybersecurity Events" (as defined below), and guidance from industry and regulatory information.

F. Access and Data Security Systems

has developed and implemented the following safeguards intended reasonably to mitigate the risks identified in the Risk Assessment.

1. Access Controls

The ***CCO/CTO*** has identified as a risk the potential misuse of legitimate but inactive user accounts, as well as the potential misuse of existing access accounts for unauthorized and malicious purposes. To limit this risk, the ***CCO/CTO*** has implemented the following access controls:

- Tempo Wealth, LLC's network infrastructure (including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and File Transfer Protocols) is the property of Tempo Wealth, LLC and are to be used for business purposes in serving the interests of Tempo Wealth, LLC and its customers in the course of normal operations.
- All network system access accounts will be reviewed and any access account that cannot be associated with a business purpose and account owner will be disabled (not deleted).
- Remote access to the network from employees' personal computers are limited to approved remote access software and Internet portals, which will be configured with the same access restrictions included herein.
- Each wireless device connected to the network must be inventoried on Attachment A, match an authorized configuration and security profile, have a documented owner and have a defined business need.
- Upon termination of any employee, contractor or agent, the access account assigned to the employee, contractor or agent will be disabled immediately, but not deleted. The electronic audit trail of the disabled account will be preserved to monitor any attempted misuse of the account.
- The network will regularly monitor the use of all active accounts, and automatically log off users after a period of inactivity not to exceed one hour.
- The network will configure screen locks on systems to limit access to unattended computer stations.
- All accounts must be supported by strong passwords that contain 8 letters, must contain at least one number, contain but capital and lower-case letters, and contain at least one special character. Passwords must be changed on a semi-annual basis and not be the same as the previous 3 passwords as a new password. Staff should also utilize two factors of authentication when possible.
- Passwords should not be shared with anyone other than Tempo Wealth, LLC's authorized administrative personnel who have been granted permission to password management.
- Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

- Monitor attempts to access deactivated accounts through audit logging.

- Restrict and audit all access to password files in the system.

2. Data Security

Physical hardware and electronic data storing or containing Personal Information and Proprietary Technology reside in many places. Protection of that hardware and data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques. The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. Accordingly, the ***CCO/CTO*** has implemented the following data security measures:

- Tempo Wealth, LLC deploys approved hard drive encryption software to all devices and systems that hold Personal Information and Proprietary Technology, including mobile and remote devices.

- Tempo Wealth, LLC prohibits employees from using third-party or personal electronic mail or storage systems (such as Google Mail, Yahoo, MSN Hotmail, etc.) to conduct Firm business or transmit or store any Personal Information or Proprietary Technology.

- Tempo Wealth, LLC employs encryption software to encrypt data in transit between networks.

- The ***CCO/CTO*** will perform annual reviews of encryption technology for updates to industry standards.

- Tempo Wealth, LLC blocks access to known file transfer and e-mail exfiltration websites, which are identified by anti-spam and Internet security software.

3. Backup Procedures

Where machines and infrastructure are compromised, the breach often changes the configurations and software. Such changes may jeopardize the effectiveness of the network systems. After a cyber-attack or other surreptitious breach of cybersecurity, Tempo Wealth, LLC may not be able to remove all aspects of the intrusion or otherwise continue with the computers that have been compromised. It is therefore necessary for Tempo Wealth, LLC to backup data regularly so that such data may be restored following a breach. Accordingly, the following procedures shall be implemented:

- Tempo Wealth, LLC's systems, including the operating system, application software, and data on each machine in the network, shall be automatically backed up on at least at least on a monthly basis.

- Backed up data should be tested on an annual basis by performing a data restoration process to ensure that the backup is properly working and all necessary systems data, software and applications can be restored.

- Ensure that backup data is properly protected via physical security or encryption where stored, as well as when such data is moved across the network. This includes remote backups and cloud services.

G. Detection of Unauthorized Access and Cybersecurity Events

The ***CCO/CTO*** seeks to employ the most recent software and technologies to detect hardware, software, malicious code and other efforts to breach cybersecurity controls, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. The ***CCO/CTO*** has adopted the following procedures to detect unauthorized access and efforts to breach Tempo Wealth, LLC's cybersecurity protocols ("Cybersecurity Events").

- Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.

- Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares.

- Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

- Employ software that scans and blocks e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business.

- Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.

- Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. [If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.]

- Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs should be archived and digitally signed on a periodic basis.

- The initial retention period for Logs shall be two months, which is estimated to be sufficient to detect a cybersecurity breach. The ***CCO/CTO*** shall continuously review and update detection times to reevaluate the retention period for logs.

- The CCO or designee will run annual reports that identify anomalies in logs. Anomalies should be documented for review by the ***CCO/CTO*** .

H. Response to Cybersecurity Events

The response function supports the ability to contain the impact of a potential Cybersecurity Event. The following are cybersecurity incident response procedures that personnel shall follow.

1. It is the responsibility of all Tempo Wealth, LLC employees to report any detected Cybersecurity Event to the CCO/CTO as soon as practicable. Such report shall include as much detailed information as possible, including the date, time and nature of the event, the system(s) breached, and the Personal Information and/or Proprietary Technology compromised. The report may be in writing or oral, but should be documents as soon as practicable by the employee or ***CCO/CTO***;

2. The ***CCO/CTO*** shall take immediate remedial measures to terminate or limit the adverse consequences of the Cybersecurity Event, including shutting down any systems impacted, blocking access to compromised customer accounts, canceling transactions or transfers of funds.

3. The ***CCO/CTO*** will conduct an assessment of the nature and scope of the incident, including (a) the manner of unauthorized access or intrusion, (b) the system(s) compromised, (c) the Personal Information and/or Proprietary Technology accessed or affected, (d) the circumstances which led to the detection of the Event, and (e) any continuing risk to ongoing operations;

4. Based on the assessment of the nature and scope of the incident, the ***CCO/CTO*** will direct and supervise all actions necessary to contain the Cybersecurity Event and prevent further unauthorized access to, or unauthorized disclosure or use of, Personal Information and/or Proprietary Technology, including coordinating with third-party services providers as necessary;

5. If the assessment of the ***CCO/CTO*** determines that Personal Information has been or will be misappropriated, the Tempo Wealth, LLC shall as soon as practicable and consistent with state and federal laws: (a) communicate the facts of the event in writing to the customer(s) affected by the Cybersecurity Event, (b) communicate to the custodians of all affected customers of the breach, (c) coordinate with the customers' custodian(s) to file the appropriate reports, such as Suspicious Activity Reports, as required by Federal and state laws; and (d) prepare a written summary of the event, the remedial measures taken, all parties informed of the event, and any risks of future events.

6. The written communication to be provided to customers affected by the Cybersecurity Event shall include all information required by applicable federal and state law, and at a minimum include:

    a. the date or dates of the event;

    b. the particular Personal Information that was compromised;

    c. the manner in which the event was detected;

    d. the remedial measures taken by the Adviser; and

    e. any measures that the customer may take to protect from further compromise.

I. Recovery from Cybersecurity Events

Following a Cybersecurity Event, Tempo Wealth, LLC shall recover operations as quickly as practicable. If the Cybersecurity Event constitutes or causes a Substantial Business Disruption, as defined by the Business Continuity Plan ("BCP"), the CCO shall implement those procedures in the BCP to recover operations. The primary functions of the recovery effort shall be directed to:

1) Executing recovery systems from backup sources to restore systems and data to pre-Event functions;

2) Updating this Policy, the BCP and any other compliance procedures to incorporate the information collected from the Cybersecurity Event and remedial response; and

3) Communicating with stakeholders, including employees, customers, regulators, vendors, and third-parties as necessary to disclose the status of the Event and recovery of operations.

J. Periodic Review of the Cybersecurity Program

In reviewing this Policy on a quarterly basis, the ***CCO/CTO*** should evaluate the sufficiency of existing controls and technologies as information is collected from operations. In each review, the ***CCO/CTO*** should proceed as follows:

Scope and Priority. The ***CCO/CTO*** identifies the Adviser's business objectives and high-level organizational priorities. For Tempo Wealth, LLC, this includes protecting Personal Information and Proprietary Technologies necessary for the delivery of advisory services to individuals, entities and private funds through several platforms.

Orientation. Once the scope of the cybersecurity program has been determined for the Adviser, the ***CCO/CTO*** should review and update the Infrastructure Inventory, consider new and existing regulatory requirements, and evaluate the existing overall risks to the business priorities.

Review the Current Cybersecurity Systems. The ***CCO/CTO*** should then review the results that are currently being achieved by existing procedures, including any Cybersecurity Events and substantial business disruptions incurred in the previous quarter(s).

Reevaluate the Risk Assessment. The ***CCO/CTO*** should reassess the existing risks given emerging information on threats and impact of previous and potential Cybersecurity Events.

Create Targeted Enhancement of Existing Cybersecurity Protocols. The ***CCO/CTO*** should incorporate addition information collected from ongoing procedures and responses to Cybersecurity Events to develop enhancements to those procedures that control network access, detect unauthorized access and respond to and recover from future Cybersecurity Events.

Determine, Analyze, and Prioritize Gaps. The ***CCO/CTO*** then must compare the current procedures and the targeted enhancements to create a prioritized action plan to address gaps, determine resources necessary to address the gaps and conduct a cost/benefit analysis of proposed enhancements.

Implement Action Plan. Based on the analysis of gaps and the cost/benefit of enhancement, the ***CCO/CTO*** will recommend to management those actions that should be taken to address gaps, if any, identified in the previous steps.

K. Vendors

Tempo Wealth, LLC has taken the following actions intended to identify potential weaknesses and vulnerabilities in the Policy as a result of the Adviser's reliance on technology-based processes maintained by Vendors:

1) Tempo Wealth LLC has evaluated existing safeguards which restrict access by Tempo Wealth, LLC employees and third-parties to technology provided by Vendors;

2) The Firm requires that each Vendor agrees in a contract to implement and maintain appropriate safeguards and measures to protect Personal Information and Proprietary Technology;

3) Each Vendor agrees in a contract to advise Tempo Wealth, LLC if there is a breach of cybersecurity procedures to protect Personal Information or Proprietary Technology.

L Consulting Resources

The ***CCO/CTO*** may retain relevant third-party forensic, legal, and other experts capable of assisting the FIrm to identify means to enhance those elements of the Policy intended to prevent, detect, and remediate Cybersecurity Events.

M Training

No less than once per year, Tempo Wealth, LLC will train relevant staff regarding the primary elements of the Policy. The training will cover, at a minimum, Tempo Wealth, LLC's legal and regulatory obligations to protect Personal Information, and a summary of the elements of the Policy intended to safeguard such Personal Information, including:

1) standards for controlling access to the network, including password protection, restricted use of mobile and external devices, and necessary minimum encryption technology for safeguarding mobile and personal devices used for access to the network;

2) procedures for identifying and reporting Cybersecurity Events to the ***CCO/CTO***;

3) restrictions on the use of Tempo Wealth, LLC's infrastructure to avoid cyber-attacks;

4) securing hardcopy files containing Personal Information and Proprietary Technology;

5) obligations of all personnel to maintain the confidentiality of Personal Information of customers; and

6) lessons learned from previous Cybersecurity Events and updated risk assessments.

N Insurance

Tempo Wealth, LLC has purchased information security insurance coverage. The coverage applies in the event of an information security incident, and is intended to defray the costs incurred by Tempo Wealth, LLC, among other things, to:

(a) Restore network security;

(b) Investigate the incident;

(c) Recover data believed to be lost as a result of the incident;

(d) Obtain legal advice regarding Tempo Wealth, LLC 's obligations arising from the incident;

(e) Respond to any business interruption resulting from the incident;

(f) Notify clients regarding the incident; and

(g) Respond to any claim brought by a regulator or client, including (with respect to the latter) any claim of breach of privacy.

ACKNOWLEDGEMENT AND ACCEPTANCE ON NEXT PAGE

ACKNOWLEDGMENT AND ACCEPTANCE

I have read the above Information Security Policy and agree to comply with the provisions contained therein.

ACCEPTED AND AGGREED TO:

Employee

By:_____

Name:_____

Date:_____