COROEBUS
WEALTH MANAGEMENT

Information Systems Security and Privacy Policy

Version 1.0

December 3, 2023

I. INTRODUCTION

Coroebus Wealth Management (CWM) is committed to providing the highest level of privacy and security to our clients' information. This Information Systems Security and Privacy Policy outlines our approach to protecting the confidentiality, integrity, and availability of all information assets within our organization.

II. SCOPE

This policy applies to all employees, contractors, vendors, affiliates and any other individuals who have access to CWM’s information systems and data.

III. INFORMATION CLASSIFICATION

CWM classifies information assets based on their sensitivity and criticality. The following classification levels are used:

1. Public Information: Information that is readily available to the public and does not require special protection
2. Nonpublic Personal Information (NPI): Information that is not available to the public but may be disclosed to specified parties for business activities
3. Confidential Information: Highly sensitive information that requires strict access controls and encryption to prevent unauthorized disclosure or misuse

IV. ACCESS CONTROL

Access to CWM's systems and data must be authorized and limited to individuals who need it to perform their job responsibilities. The following access control measures are in place:

1. Unique User IDs: Each user is assigned a unique user ID, and password-based authentication is used to grant access to systems
2. Role-Based Access Control (RBAC): Access privileges are assigned based on job roles and responsibilities. Access permissions are regularly reviewed to ensure they align with the principle of least privilege
3. Privileged Access Management: Special controls are in place to manage and monitor the access rights of privileged users, such as system administrators
4. Multi-Factor Authentication: Strong authentication mechanisms, such as biometrics or hardware tokens, are utilized to enhance access security for sensitive systems and data

V. DATA PROTECTION AND ENCRYPTION

CWM employs encryption technologies to protect sensitive information during transmission and storage. The following encryption practices are implemented:

1. Transport Layer Security (TLS): Strong encryption protocols are used to protect data in transit over public networks
2. Data-at-Rest Encryption: All sensitive data stored on portable devices and servers is encrypted to prevent unauthorized access in the event of loss or theft
3. Backup Encryption: Data backups are encrypted to ensure the confidentiality and integrity of information

VI. INCIDENT MANAGEMENT

In the event of a security incident or breach, CWM has implemented an incident management process to minimize damages and ensure a swift response. The process includes the following steps:

1. Incident Detection and Reporting: Any suspected security incidents or breaches must be reported immediately to the designated security team or IT department
2. Incident Response: A predefined incident response plan is activated to address the incident. This includes containment, eradication, recovery, and forensic analysis
3. Lessons Learned: After an incident is resolved, a thorough analysis is conducted to identify root causes and implement corrective actions to prevent similar incidents in the future

VII. PRIVACY AND COMPLIANCE

A. PRIVACY PRACTICES

CWM is required by law to inform their clients of their policies regarding privacy of client information. We are bound by professional standards of confidentiality that are even more stringent than those required by law. Federal law gives customer the right to limit some but not all sharing of personal information. It also requires us to tell you how we collect, share, and protect your personal information. Key privacy practices include:

1. Data Access and Consent: Personal information is collected and accessed based on explicit consent obtained from clients and in accordance with applicable laws
2. Data Retention: Personal data is retained only for as long as necessary and securely disposed of when no longer needed
3. Privacy Training: Employees receive regular training on privacy policies, regulations, and best practices to ensure adherence to privacy principles

B. NONPUBLIC PERSONAL INFORMATION (NPI)

CWM collects NPI about you that is either provided to us by you or obtained by us with your authorization. This can include but is not limited to your Social Security Number, Employer Identification Number, Date of Birth, Banking Information and Financial Account Numbers and/or Balances, Sources of Income, Credit Card Numbers or Information. When you are no longer our customer, we may continue to share your information as described by this policy. Associated parties to whom we disclose personal information:

1. For everyday business purposes; such as to process your transactions, maintain your account(s), or respond to court orders and legal investigations, or report to credit bureaus
2. For our marketing; to offer our products and services to you
3. For Joint marketing with other financial companies
4. For our affiliates' everyday business purposes; information about your transactions and experiences
5. For non-affiliates to market to you

C. OPTING OUT OF NPI SHARING

Clients may opt out of sharing information for joint marketing to other financial companies, to our affiliates and to non-affiliates. If you are a new customer we may begin sharing your information on the day you sign our agreement. When you are no longer our customer, we may continue to share your information as described in this policy. However, you can contact us at any time to limit our sharing.Federal law allows you the right to limit the sharing of your NPI by "opting out" of the following:

1. Sharing for affiliates' everyday business purposes – information about your creditworthiness
2. Sharing with affiliates who use your information to market to you

3. Sharing with non-affiliates to market to you. State laws and individual companies may give you additional rights to limit sharing. Please notify us immediately if you choose to opt out of these types of sharing

Affiliates – companies related by common ownership or control. They can be financial and nonfinancial companies. Non-affiliates – companies not related by common ownership or control. They can be financial and nonfinancial companies. Joint marketing – a formal agreement between non-affiliated financial companies that together market financial products or services to you.

VIII. SECURITY AWARENESS AND TRAINING

CWM acknowledges the importance of security awareness and training to maintain a secure environment. All employees undergo training on information security policies and procedures to promote a security-conscious culture within the organization.

IX. POLICY REVIEW AND UPDATE

This Information Systems Security and Privacy Policy will be reviewed periodically to ensure its effectiveness and alignment with changing technology, legal, and business requirements. Updates to the policy will be communicated to all relevant personnel.

X. POLICY VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination and legal prosecution if necessary.

11. POLICY ACCEPTANCE

By accessing CWMs information systems or handling sensitive data, all employees, contractors, vendors, affiliates and authorized users agree to comply with this Information Systems Security and Privacy Policy.

END OF POLICY