Statement of Policy

The objective of Capita Financial Network ("Capita", "The Company") in the development and implementation of this comprehensive Written Information Security Policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information ("PII") of customers, clients and employees as well as sensitive company information that could be harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive company information.

The use of the term ***employees*** *will include all of The Company's owners, partners, managers, employees, all independent contractors, temporary employees and interns.*

Purpose of Policy

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of PII of customers, clients, employees or vendors as well as sensitive company data which includes emails, confidential company information (i.e. company proprietary information and highly sensitive information, etc.), employee information, payroll and the like;
2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to The Company.

Scope of Policy

In formulating and implementing the WISP, Capita Financial Network has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive company data.
2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.
3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.
4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.
5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The following safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive company data.

Administrative Safeguards

Security Officer

The Company has designated Scott Watko, Chief Compliance Officer ("CCO"), as the Security Officer responsible for implementing, supervising, and maintaining the WISP.

The Security Officer's key duties include:

- Implementing the WISP and all associated Security Safeguards.
- Providing training on data security to all employees with access to PII and sensitive company data, including annual refresher training and onboarding training for new hires.
- Monitoring compliance with the WISP safeguards and employee adherence.
- Assessing Third-Party Service Providers' security practices, ensuring contracts require appropriate protections for PII and sensitive data.
- Reviewing and updating security measures at least annually or when significant changes to business practices occur.
- Investigating, reviewing, and responding to all actual or suspected security incidents.

Security Management

All security measures shall be reviewed at least annually, or whenever a material change in business practices may expose PII or sensitive company data to new risks. This includes conducting a formal security risk assessment, documenting findings, and implementing recommended improvements.

Risk Assessment Process:
Under the direction of the Security Officer (or delegate), Capita will perform an annual WISP security risk assessment that:

- Identifies known and reasonably foreseeable internal and external threats.
- Evaluates the likelihood and potential impact of these threats.
- Assesses the adequacy of current administrative, technical, and physical safeguards.
- Assigns risk severity ratings and sets timelines for remediation of significant risks
- Is documented, reviewed by senior compliance personnel, and retained for at least five years.

The Security Officer is responsible for conducting the review, communicating results and recommendations to the executive team, and documenting any material changes to the WISP or related procedures.

Minimal Data Collection

The Company collects PII from clients, customers, and employees only as necessary to conduct legitimate business transactions and comply with all applicable federal, state, and local regulations.

Capita collects PII solely to:

- Fulfill fiduciary and regulatory obligations.
- Deliver investment advisory or insurance services.
- Meet contractual or legal requirements.

Data collection practices are reviewed at least annually to ensure ongoing compliance with regulatory requirements.

Information Access

Access to records containing PII and sensitive company data is restricted to personnel whose job functions require such access for legitimate business purposes. Pre-employment screening is conducted to help safeguard this information.

Access controls apply to electronic systems, physical files, and environments storing PII or sensitive data and must:

- Be limited to personnel with a legitimate, role-based business need.
- Be audited as needed to verify appropriate access levels.
- Be revoked immediately upon employee termination or job function changes.
- Be logged and regularly reviewed to detect unauthorized access.

The CCO or delegate maintains records of all access approvals and revocations, and oversees changes to access privileges. Access attempts may be monitored periodically to ensure compliance.

Employee Termination

Upon termination of employment or contract (voluntary or involuntary), Capita requires immediate revocation of all access to PII and sensitive company data, and return or secure deletion of all related materials in the former employee's possession.

Requirements for Terminated Employees:

- Return all records containing PII or sensitive data in any form, including information on laptops, portable devices, media, files, records, and work papers.

- Surrender all keys, IDs, access codes, business cards, and any other items granting access to company premises or systems.
- Remote electronic access—including voicemail, email, internet, and passwords—must be disabled immediately.

Offboarding Procedures (completed on the same business day or as soon as feasible):

- Revoke all physical and digital access credentials (network accounts, email, file shares, third-party platforms).
- Retrieve all company-issued equipment and physical documents containing sensitive or proprietary data.
- Instruct terminated employees to return or confirm destruction of any business data stored on personal devices.
- Disable remote access, email forwarding, and voicemail systems.
- Conduct an offboarding checklist review involving the Compliance, HR, and Operations departments.
- Maintain written records of access revocation and asset recovery in the employee's compliance file.

Security Training

All personnel—including owners, partners, managers, full-time employees, interns, independent contractors, and temporary workers—with access to PII or sensitive company data must complete mandatory information security training.

Training Requirements:

- Timing: New hires must complete training within 10 days of onboarding and all employees must complete training at least annually.
- Content: Training covers key security topics such as phishing awareness, password best practices, remote work safeguards, incident reporting, and proper data handling.
- Evaluation: Employees must pass an assessment or knowledge check to demonstrate understanding.
- Documentation: The CCO (or delegate) will maintain training records, including dates and assessment results.
- Updates: Additional training may be required to address emerging threats, incidents, or regulatory changes.

WISP Distribution

A copy of the WISP shall be provided to all current employees and new hires on their first day of employment. Employees are responsible for electronically attesting that they have received and agree to comply with the WISP.

The CCO is responsible for:

- Distributing the WISP to all supervised persons and employees upon hire and whenever material updates occur.
- Ensuring each recipient electronically attests to receipt and understanding of the WISP.
- Storing the current WISP in a centralized, accessible location (e.g., compliance intranet or secure drive).
- Providing access to the most current WISP version upon request.
- Maintaining a log of all acknowledgments and re-circulating the policy following significant regulatory, operational, or procedural changes.

Contingency Planning

All systems storing PII and/or sensitive company data must be backed up at least nightly. Backups must be encrypted and stored offsite to ensure data security and availability.

Capita maintains a documented Business Continuity Plan ("BCP") that outlines roles, responsibilities, and procedures to restore access to PII, sensitive data, and critical operational systems in the event of a disruption, including cybersecurity incidents, natural disasters, or infrastructure failures.

Key elements include:

- Nightly encrypted backups of core business systems and client records.
- Secure offsite or cloud-based storage of backups to enable rapid restoration.
- Defined Recovery Time Objectives ("RTOs") and Recovery Point Objectives ("RPOs") for mission-critical systems, subject to the capabilities and limitations of third-party vendors' platforms.
- Annual testing of disaster recovery capabilities and documentation of outcomes.
- A clear incident response communication plan for notifying internal teams, custodians, or regulators if material service disruptions or data losses occur.
- Assignment of responsibility to the CCO for coordinating periodic reviews and improvements to the plan.

Security Incident Procedures & Emergency Operations

Capita maintains documented procedures to respond promptly and effectively to security incidents and emergencies involving personal data, confidential business information, or critical systems.

Security Incident Definition:
A security incident is any unauthorized access, use, disclosure, alteration, or destruction

of personal or company data, or any event that compromises the availability, confidentiality, or integrity of systems managing such data.

Incident Reporting:
All employees, contractors, and supervised persons must immediately report any actual or suspected security incident to their supervisor, the CCO, or the designated Security Officer.

Reportable Incidents Include, but Are Not Limited To:

- Unauthorized access to client, firm, or system data.
- Phishing, malware, or ransomware attacks.
- Loss or theft of devices containing sensitive or personal information.
- Accidental disclosure or exposure of sensitive information.
- Account compromise or other suspicious activity

Incident Response Workflow
Upon Receiving a Report, the Security Officer Will:

- Log the incident in the firm's Security Incident Register.
- Initiate an investigation to assess the scope, severity, and impact.
- Implement containment, mitigation, and remediation actions.
- Determine legal or regulatory obligations, including whether notification to clients, custodians, or authorities is required.
- Notifications will be made within applicable timeframes (e.g., SEC's 72-hour rule, state data breach laws).
- Conduct a root cause analysis to identify and address underlying issues.
- Update policies or controls as needed to prevent recurrence.

Documentation and Follow-Up:

- All incidents must be documented using the firm's Security Incident Report Form.
- Incident records will be reviewed annually by senior leadership as part of compliance oversight and to inform updates to the firm's WISP.

Emergency procedures also include up-to-date employee and critical vendor contact information, key account details, and operational protocols to ensure business continuity.

Data Sensitivity Classification

To protect the integrity and privacy of information, Capita treats all data as *Confidential* by default. Formal data classification is performed on an as-needed basis—most

critically during incidents such as a data breach or security assessment, when the nature and sensitivity of the affected data must be determined.

Capita's Data Classification Levels

These levels provide a framework to categorize data based on sensitivity, regulatory requirements, and potential impact. While not every piece of data is pre-assigned a classification, these categories guide our response and handling protocols:

- Confidential: Data that, if accessed or disclosed without authorization, could cause significant harm to clients, employees, or the firm. This includes PII such as Social Security Numbers and account numbers, firm financials, investment strategies, passwords, client contracts, and regulatory correspondence. When identified, this data must be encrypted both in storage and in transit and access is restricted to authorized personnel only.
- Internal Use Only: Non-public information intended for use within Capita, such as HR policies, training materials, internal procedures, and system configurations. This data may be shared internally, but not externally without prior approval.
- Public: Information explicitly approved for public disclosure, including website content, marketing materials, and regulatory filings like Form ADV.

All personnel are expected to treat all data with a high degree of care and default to a *Confidential* handling posture unless otherwise directed. The CCO is responsible for reviewing and updating the classification framework periodically. New systems, forms, and data types will be assessed and classified when necessary—particularly during the approval process or in response to a data incident.

Third Party Service Providers

Any service provider or individual ("Third Party Service Provider") with access to files containing PII or sensitive company data must protect that information in accordance with The Company's standards. Examples include vendors providing off-site data backup, website hosting, credit card processing, record storage, IT support, or contractors with authorized access.

Requirements for Third Party Service Providers with Access to PII or Sensitive Data:

- Complete and sign Capita's Due Diligence Questionnaire that includes:
  - A documented security risk assessment completed prior to engagement.
  - Confidentiality provisions.
  - Information security controls aligned with industry standards.
  - Breach notification timelines and cooperation clauses.
- Undergo annual reassessments to verify ongoing compliance.

- Notify Capita within 72 hours of any actual security incidents involving company or client data.

The CCO (or designee) will maintain and annually review a list of all vendors with access to protected data as part of the compliance program.

Physical Safeguards

Facility Access Controls

Capita implements physical safeguards to protect PII and sensitive company data at all office locations and any location where such data is accessed, stored, or processed. These safeguards are designed to prevent unauthorized physical access, ensure data security, and support compliance with applicable laws and regulations.

The following physical security protocols apply:

- Facility Access Control: Office entry is restricted and managed through Alta Open, a secure keycard app issued only to authorized personnel. After-hours access is limited and logged where applicable.
- Secured Systems and Equipment: All systems and devices that access or store PII or sensitive data must be physically secured when unattended. Portable equipment and storage media must be locked or otherwise secured.
- Locked Storage: Paper records and physical files containing PII or proprietary company data must be stored in locked cabinets when not in use.
- Clean Desk Policy: Employees are required to maintain a clean desk environment. No confidential information may be left unattended or unsecured during or outside of business hours.
- Visitor Restrictions: Visitors are not permitted in areas where sensitive data is stored or accessed unless escorted by authorized personnel. Access must be documented and monitored.
- Secure Disposal: Documents containing sensitive or confidential information must be shredded or securely destroyed when no longer required.
- Service Provider Oversight: Cleaning crews and third-party service providers must be screened and supervised when working in areas containing sensitive data.
- Remote Locations: Remote offices and offsite locations are subject to periodic audits by the CCO or their delegate.
- Access Records: The Security Officer maintains a record of all physical security access credentials, including lock combinations, passcodes, and keys, along with a list of employees authorized to access secured areas and systems.

These physical security measures are an essential part of Capita's broader information security program and are designed to ensure the confidentiality, integrity, and availability of sensitive data across all locations.

Network Security

Capita implements a range of security safeguards to protect PII, sensitive company data, and critical systems from unauthorized access, data breaches, and malicious activity. These safeguards apply across all office locations, remote environments, and devices connected to the Capita network.

Key security controls include:

- System Isolation and Firewalls: Systems that access or store PII and sensitive data are logically segmented and protected by commercial-grade firewalls and router configurations to prevent unauthorized external access.
- Endpoint Protection: All company-managed devices are equipped with up-to-date antivirus and anti-malware tools. Operating systems and applications must be regularly patched in accordance with vendor recommendations or IT directives.
- Encryption and Device Security: All portable devices must use full-disk encryption and be physically protected when in transit or unattended. Devices must meet Capita's current security standards to connect to the network.
- Device Compliance Checks: Any device accessing Capita's network or systems is subject to periodic audits to ensure compliance with security requirements. Non-compliant devices may be denied access until remediated.
- Remote Access Controls: Remote access (e.g., home offices, mobile devices) to the company's network must be established through a secure VPN and require multi-factor authentication ("MFA").
- Role-Based Access: Network access is granted based on job responsibilities. Administrative privileges are limited to authorized personnel only.
- Wireless Security: Business Wi-Fi networks must be password-protected, encrypted using WPA2 or higher, and regularly reviewed for unauthorized access or vulnerabilities.
- Vulnerability Management: Capita performs periodic vulnerability scans and device audits to identify and remediate security risks across its network and infrastructure.
- Environmental Protections: Servers and critical network equipment must be housed in environmentally controlled, secure locations to protect against physical damage.
- Log Monitoring: Network activity and system access logs are captured and reviewed regularly by the CCO or designated IT partners to detect unauthorized access or suspicious behavior.

These controls form the foundation of Capita's cybersecurity program and ensure ongoing protection of firm and client data across all systems and environments.

Technical Safeguards

Access Control

Access to PII, sensitive company data, systems, and applications is restricted based on job function, ensuring users have only the minimum access necessary to perform their responsibilities. Only approved and active users with unique login credentials are authorized access; shared accounts are strictly prohibited.

Capita enforces the following access control and data protection procedures:

- All employees are assigned unique user accounts and passwords tied to their roles.
- Access to sensitive or client-specific data requires explicit approval from the CCO or a designated manager.
- Role-based access permissions are defined, maintained, and limited to the minimum necessary for job responsibilities.
- Access rights are reviewed at least annually and upon job changes, transfers, or termination.
- Upon employee separation, all system access must be revoked on the same business day.
- All system access requests and changes are documented and logged.
- Automatic session timeouts, lock screens, and logoff procedures are implemented across all endpoints and systems to prevent unauthorized access.
- A strong password policy is enforced, requiring complex passwords (minimum 12 characters with alphanumeric and symbol requirements), regular expiration, and prevention of reuse.
- All access attempts are logged and reviewed regularly for suspicious activity as part of routine monitoring.

Computer Use

All Capita employees are provided with a Equipment and IT Use Policy, which outlines the acceptable and unacceptable use of Capita's computing resources. Employees are required to acknowledge and sign this policy upon hire and annually thereafter.

Capita personnel must use company computing devices and systems in a manner consistent with their job responsibilities and Capita's Written Information Security Policy.

Violations of this policy may result in disciplinary action, up to and including termination.

Data Disposal

Capita ensures that written and electronic records containing PII or sensitive company data are securely destroyed or deleted at the earliest opportunity, consistent with business needs and legal or regulatory retention requirements.

Data disposal procedures include:

- Physical Records: Paper documents containing PII or confidential business information must be shredded using cross-cut shredders or securely destroyed by an approved third-party vendor.
- Electronic Data: In the rare instance that files must be permanently deleted, it will be done using secure deletion tools to prevent recovery. Decommissioned devices must be securely wiped, degaussed, or destroyed under the supervision of Capita's IT team or a vetted vendor.
- Retention Schedule: Unless otherwise required by law or regulation, records will be retained for a minimum of five years. After this period, they must be securely disposed of.
- Vendor Oversight: Third-party vendors used for data destruction must sign Capita's Due Diligence Questionnaire and, when applicable, provide a certificate of destruction.
- Documentation: Destruction of high-sensitivity records must be logged and retained by the CCO for at least five years.

The CCO is responsible for overseeing the implementation of secure disposal procedures and ensuring that all supervised persons understand their obligations for protecting data throughout its lifecycle.

System Activity Review

Capita maintains both technical and procedural controls to ensure that all systems storing or accessing PII and sensitive company data are continuously monitored for unauthorized or abnormal activity.

Key requirements include:

- System Logging: All systems containing client or firm-sensitive data must log and store user activity. This includes CRM platforms, email systems, custodian portals, compliance systems (e.g., MessageWatcher), and firm-managed file servers.

- Periodic Review: System activity logs are reviewed at least monthly by the CCO or a designated IT/compliance delegate as part of Capita's ongoing compliance and cybersecurity programs.
- Review Focus: Log reviews are designed to detect:
  - Unauthorized access attempts.
  - Logins from unrecognized devices or IP addresses.
  - After-hours or anomalous activity.
  - Repeated failed login attempts.
- Incident Response: Any findings of unauthorized access are documented in a System Activity Review Log. Material anomalies are escalated to the appropriate incident response procedures and reported to the Data Security Coordinator.
- Retention Requirements: All system logs must be retained for a minimum of three years or longer if required by regulation.
- Automation: Automated alerts may be enabled for critical systems where available (e.g., CRM, Orion, Schwab, Microsoft 365) to support real-time threat detection.

Encryption

To protect PII and sensitive company data, Capita requires encryption for data when stored on portable devices or transmitted over public or wireless networks.

Capita's encryption standards and practices include:

- Backups: All data backups—whether stored onsite or transferred to offsite or cloud environments—must be encrypted throughout their lifecycle.
- Cloud Services: Only Capita-approved cloud platforms may be used for storing or accessing sensitive data. These platforms must support encryption for both data at rest and in transit. Use of unapproved cloud storage or collaboration tools is not allowed.
- Key Management: Encryption keys must be securely stored and managed with access restricted to authorized personnel. Shared encryption keys are prohibited unless explicitly documented and protected.
- Monitoring and Enforcement: The CCO or designated IT provider is responsible for verifying compliance with encryption requirements through periodic checks and enforcing remediation where necessary.

Capita is committed to maintaining encryption protocols that meet or exceed industry standards to ensure the confidentiality and integrity of sensitive data.

Management of Policy

The management and oversight of this policy, including key dates and approvals, are documented as follows:

Last Review Date: 08/18/2025
Approved by: Scott Watko