MTradecraft, LLC

Privacy, Information Security, and Incident Response Policy

Document	Version	Effective Date	Owner	Supersedes
Privacy, Information Security, and Incident Response Policy	1.1	August 4, 2026	Brian Hahn, Principal	v1.0 (June 3, 2026)

1. Purpose and Scope

This Policy establishes how MTradecraft, LLC ("MTradecraft," "we," "our") protects the confidentiality, integrity, and availability of client information entrusted to us in the course of providing cybersecurity, compliance, and corporate intelligence services.

MTradecraft serves SEC-registered investment advisers and other financial institutions that are themselves "covered institutions" under SEC Regulation S-P (17 C.F.R. § 248). As a service provider to covered institutions, MTradecraft has designed this Policy to satisfy the service provider oversight, safeguarding, disposal, and incident notification expectations of amended Regulation S-P, and to support our clients' compliance-program and recordkeeping obligations under Advisers Act Rule 206(4)-7 and Rule 204-2.

This Policy applies to all MTradecraft personnel, contractors, systems, devices, and physical workspaces used to deliver client engagements, and to all client information regardless of format (electronic, paper, or verbal).

2. Definitions

Client Information — Any record, communication, finding, configuration, scan result, document, or derivative work containing or referencing a client's nonpublic information, regardless of whether it identifies an individual.

Sensitive Customer Information — As defined under Regulation S-P § 248.30(d)(9): any component of customer information that, alone or in conjunction with any other information, could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.

Security Incident — Any event, or reasonably suspected event, involving unauthorized access to, acquisition of, use of, modification of, or disclosure of client information or the systems that process it.

Breach — A Security Incident confirmed to have resulted in, or reasonably likely to result in, unauthorized access to or use of client information.

Covered Institution — A client that is itself subject to Regulation S-P (broker-dealer, registered investment adviser, investment company, transfer agent, or funding portal).

3. Privacy Policy

MTradecraft treats client information as carefully as we treat our own — responsibly, securely, and with full respect for client ownership rights.

3.1 Data Ownership

We do not own client data; the client does. All work product, evidence, scan output, and intelligence we generate on behalf of a client is the property of that client, subject to the engagement agreement. MTradecraft retains copies only as needed to deliver services and to satisfy our own recordkeeping obligations.

3.2 No Data Sales, No Hidden Agendas

MTradecraft will never sell, trade, license, or otherwise monetize client information. Our business model is direct: we provide professional cybersecurity and intelligence services at transparent prices. We have no relationships with advertisers, IT resellers, MSPs, or outsourced service providers that could compromise client confidentiality.

3.3 No Sharing With Affiliates or Non-Affiliated Third Parties

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

MTradecraft does not share client nonpublic personal information with affiliated or non-affiliated third parties for marketing purposes. We do not engage in joint marketing arrangements that would require Regulation S-P opt-out notices on behalf of any client.

The only circumstances in which we disclose client information are:

- To the client itself or persons the client authorizes in writing;
- To the extent strictly required to perform the contracted service (for example, narrowly scoped vendor lookups against public registries);
- As required by law, valid subpoena, or court order, in which case we will, where legally permitted, notify the client before disclosure.

3.4 Vendor and Subcontractor Standards

MTradecraft does not use general-purpose consumer cloud productivity suites for the storage or processing of client information. Any vendor that receives, hosts, or has the potential to access client information is reviewed for: encryption at rest and in transit, access controls, breach notification commitments, U.S. data residency, and SOC 2 Type II (or equivalent) attestation where applicable.

3.5 Material Nonpublic Information (MNPI)

In the course of an engagement, MTradecraft may be exposed to a client's material nonpublic information — including nonpublic details of the client's security posture, business operations, holdings, or personnel. MTradecraft:

- Treats all MNPI encountered during an engagement as Client Information subject to every safeguard in this Policy;
- Does not trade in securities on the basis of, and does not communicate to any other person, MNPI obtained through an engagement, consistent with Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder;
- Uses client information solely to perform the contracted service, and for no other purpose;
- Restricts engagement information to personnel with a documented need to know (currently the principal only); and
- Treats any suspected misuse of MNPI as a Security Incident subject to Section 5 of this Policy.

4. Information Security Program

Protecting client information is core to our mission. As a cybersecurity advisory firm, we apply a defense-in-depth approach with administrative, technical, and physical safeguards reasonably designed to (i) ensure the security and confidentiality of client information, (ii) protect against anticipated threats or hazards, and (iii) protect against unauthorized access to or use of client information that could result in substantial harm or inconvenience.

4.1 Platform and Endpoint Security

- All MTradecraft endpoints, workstations, and servers used to access, process, or store client information are hardened against the firm's internal baseline, which is derived from recognized industry benchmarks and reviewed at least annually.
- Hardening includes, at minimum: removal of unnecessary services and software, restriction of administrative privileges, enforcement of host-based firewall and endpoint protection controls, application allow-listing where feasible, secure boot configuration, and full-disk encryption.
- Endpoints used to access client environments are logically and operationally separated from endpoints used for general business administration and research.
- Mobile devices are not used to store client work product or evidence.
- Compartmentalized workflows are used to separate client engagement data from administrative, research, and general-purpose activity.

4.2 Encryption Standards

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

- All data in transit is encrypted using TLS 1.2 or 1.3 with modern cipher suites.
- All client data at rest is encrypted using AES-256 or a stronger industry-accepted algorithm.
- Disk-level and volume-level encryption is applied to all MTradecraft endpoints holding client information.
- Encryption keys are protected using industry-accepted key management practices, including key wrapping and strict access restriction.
- Remote access to client environments uses modern, encrypted VPN protocols layered over zero-trust overlay networking.

4.3 Access Controls

- Only authorized MTradecraft personnel with a documented business need-to-know are permitted to access client information.
- Access requires multi-factor authentication; phishing-resistant authentication methods are used wherever supported.
- MTradecraft has not granted, and does not anticipate granting, third-party access to client data. If such access ever becomes necessary, it will be subject to written client consent and a formal access record.
- Administrative privileges are tightly restricted and segregated from day-to-day operational accounts.

4.4 Data Architecture and Storage

- Client information is stored on encrypted, access-controlled storage under MTradecraft's direct control.
- MTradecraft does not store client information in consumer cloud storage services.
- Email containing client information is retained in protected local archives on encrypted storage and is not synchronized to third-party search or AI indexing services.

4.5 Artificial Intelligence and Large Language Model Handling

MTradecraft recognizes that uncontrolled use of cloud-based generative AI services creates material confidentiality, recordkeeping, and regulatory risks for financial institutions. MTradecraft's use of AI is therefore subject to the following controls:

- Local-only AI for client data. Any AI or large language model work that involves client information is performed using local AI models running on MTradecraft-controlled, hardened infrastructure that does not transmit client information to any external service, application programming interface, or third-party model provider.
- No training on client data. Client information is not, and will not be, used to train, fine-tune, or otherwise improve any third-party AI model. Local models are not configured to retain client inputs as training data.
- Air-gapped inference where warranted. Where the sensitivity of a client engagement requires it, AI inference is performed on isolated systems with no external network connectivity for the duration of the analysis.
- Cloud AI services. External, cloud-hosted AI services may be used for general research, drafting, and administrative tasks that do not involve client information. Client information is not submitted to such services. Where MTradecraft uses an enterprise tier of an external AI service, contractual terms restricting training, retention, and human review are in place.
- AI output is reviewed. AI is used as an analytical assistant, not as a source of authoritative findings. All AI-generated content that informs a client deliverable is reviewed and validated by the principal before inclusion.
- Governance mapping. MTradecraft's internal AI use is governed against recognized AI security control frameworks (including the SANS Critical AI Security Controls) and is mapped to Advisers Act Rule 206(4)-7 supervisory expectations. The same methodology informs the AI governance assessments MTradecraft performs for clients.

4.6 Operational Security

- Security patching and system hardening are performed on a regular cadence and after any vendor advisory of high or critical severity.

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

• MTradecraft performs recurring external vulnerability scans and risk assessments of its own internet-facing infrastructure, using the same tooling and methodology deployed in client CRVT engagements; findings are remediated and documented.

• Connections to client environments are logged and monitored; anomalous activity is reviewed promptly.

• Backups of MTradecraft systems are encrypted and stored offline.

• Removable media is not used for client information, except firm-controlled encrypted media used for offline evidence storage and backup; ad hoc or personal removable media is prohibited, and all media is subject to the disposal controls in Section 4.8.

• Physical workspaces used to process client information are access-controlled; screens are positioned to prevent shoulder-surfing; documents are stored in locked containers when not in use.

• Devices used for client work are not shared with family members or other parties.

4.7 Personnel Security

• MTradecraft is operated by its principal, Brian Hahn, who performs all client work. There are no employees with access to client information at this time.

• Any future personnel will be subject to written confidentiality obligations, background screening appropriate to the role, and documented onboarding/offboarding procedures.

• Subcontractors, if engaged, are subject to written confidentiality and information security obligations no less protective than those in this Policy.

4.8 Disposal of Client Information

• Electronic client information is securely deleted using cryptographic erasure or multi-pass overwrite at the end of the applicable retention period.

• Storage media that has held sensitive client information is physically destroyed at end of life.

• Paper records containing client information are cross-cut shredded.

• Disposal activities are logged.

4.9 Culture of Security

MTradecraft embraces a “trust but verify” philosophy. Security awareness is built into daily operations. We are, by design, cautious — “paranoid” in the healthy sense — because our role is to anticipate threats before they arise.

5. Incident Response Program

In accordance with SEC Regulation S-P § 248.30(a)(3), MTradecraft maintains a written Incident Response Program reasonably designed to detect, respond to, and recover from unauthorized access to or use of client information.

5.1 Response Phases

Upon identification of a Security Incident, MTradecraft executes the following phases:

• Detect & Triage. Confirm the indicators, identify affected systems and data, and classify severity.

• Contain. Isolate affected systems, rotate credentials, revoke sessions and tokens, and block adversary persistence.

• Assess Scope. Determine the nature and scope of the incident, the categories of client information involved, and which clients are or may be affected.

• Notify (see Section 5.2). Provide the required notifications to affected clients within the timeframes set forth below.

• Eradicate & Recover. Remove the root cause, validate clean state, and restore affected services.

• Post-Incident Review. Conduct a documented lessons-learned exercise; update controls, procedures, and this Policy where warranted.

5.2 Client Notification Timing (Regulation S-P Service Provider Standard)

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

Because MTradecraft is a service provider to Regulation S-P covered institutions, our clients are required by 17 C.F.R. § 248.30(a)(5)(i) to oversee their service providers through policies and procedures reasonably designed to ensure that service providers notify them of a breach in security as soon as possible, but no later than 72 hours after becoming aware that the breach has occurred (§ 248.30(a)(5)(i)(B)). MTradecraft commits to that standard as follows:

MTradecraft will notify each affected client as soon as possible, and in no event later than seventy-two (72) hours, after becoming aware that a breach in security has occurred resulting in unauthorized access to, or use of, that client's information on a system maintained by MTradecraft.

The regulatory trigger is MTradecraft becoming aware that a breach in security has occurred. MTradecraft voluntarily applies an earlier, more protective trigger: the 72-hour clock starts when MTradecraft has a reasonable basis to conclude that such a breach has occurred or is reasonably likely to have occurred. Initial notification is not delayed pending complete root-cause analysis; supplemental notifications follow as facts develop.

5.3 Content of Notification

Initial notification to the affected client will include, to the extent then known:

- Date and approximate time MTradecraft became aware of the incident;
- Brief description of the nature of the incident and how it was identified;
- The MTradecraft systems and the categories of client information involved or reasonably likely to be involved;
- The clients or customer information sets affected or reasonably likely to be affected;
- Containment and remediation actions taken or in progress;
- MTradecraft point of contact for follow-up and coordination;
- Anticipated cadence for status updates.

5.4 Method of Notification

Initial notification will be made by direct telephone contact to the client's designated incident contact, followed by written confirmation via encrypted email or secure portal within the 72-hour window. Each client engagement establishes a designated incident contact and escalation path at engagement kickoff.

5.5 Coordination With Client's Customer Notification Obligations

Where the affected client is itself a covered institution under Regulation S-P, the obligation to ensure affected individuals are notified rests with the client (§ 248.30(a)(5)(iii)): notice must be provided as soon as practicable, and not later than 30 days after the client becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred (§ 248.30(a)(4)(iii)). MTradecraft will support its client's notification effort by providing evidence, scoping information, and timeline documentation, but will not deliver customer-facing notices on the client's behalf unless specifically engaged in writing to do so.

5.6 Recordkeeping

MTradecraft maintains written records of all Security Incidents, including detection, classification, scope assessment, notifications made (including date, time, recipient, and content), containment and remediation actions, and post-incident review findings. These records are retained for a minimum of five (5) years.

5.7 Testing

The Incident Response Program is tested at least annually through tabletop exercises and is reviewed following any actual incident or any material change to MTradecraft's systems, services, or threat environment.

6. Recordkeeping and Retention

MTradecraft retains the following records for a minimum of five (5) years, the first two (2) in an easily accessible location:

- This Policy and all prior versions, with effective dates;

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

- Risk assessments and threat detection process documentation performed by MTradecraft;
- Vendor due diligence files supporting Section 3.4;
- Access logs for systems holding client information;
- Incident records described in Section 5.6;
- Client notifications and acknowledgments;
- Annual policy review attestations and tabletop exercise records;
- Training and awareness records for any personnel.

7. Governance and Review

- This Policy is owned by the Principal of MTradecraft, who serves as the firm's information security and privacy officer.
- This Policy is reviewed at least annually and after any material change in MTradecraft's services, systems, regulatory environment, or following any reportable Security Incident.
- Changes are version-controlled and dated. Clients with active engagements may request a copy of the then-current Policy at any time.

8. Vendor Due Diligence Questionnaire (DDQ) Response Summary

The following table summarizes MTradecraft's position on common DDQ items requested by SEC-registered investment advisers and other financial institutions assessing service providers under Regulation S-P, Rule 206(4)-7, and related supervisory frameworks. Clients may request supporting evidence for any item.

DDQ Topic	MTradecraft Response / Position
Firm Overview	MTradecraft, LLC — Texas limited liability company, headquartered in Dallas/McKinney, Texas. Sole principal: Brian Hahn. Independent boutique cybersecurity compliance and corporate intelligence consultancy. No parent, affiliates, or external investors.
Services Provided	Cyber Risk Vulnerability Threat (CRVT) assessments; Remote CISO advisory; M365/Azure configuration audits; vendor due diligence; incident response advisory; FieldCraft security awareness training; corporate intelligence and OSINT services.
Regulatory Framework	Services are scoped to support client compliance with SEC Rule 206(4)-7, Rule 204-2, Regulation S-P (as amended 2024), Regulation S-ID, and applicable state privacy laws. MTradecraft itself is not a registered investment adviser.
Types of Client Data Received	Network configuration data, vulnerability scan output, policy documents, M365/Azure tenant configuration, OSINT and breach exposure findings. MTradecraft does not require access to customer PII, account numbers, or trading records to perform its services.
Data Storage Location	All client data is stored on encrypted endpoints and air-gapped or access-controlled storage under MTradecraft's direct physical control in the United States. No consumer cloud storage. No offshore data hosting.
Encryption at Rest	AES-256 (or stronger industry-accepted algorithm) full-disk and volume-level encryption on all endpoints and storage holding client information.
Encryption in Transit	TLS 1.2/1.3 with modern cipher suites. Client environment access via modern encrypted VPN protocols over zero-trust overlay networking.
Authentication	Multi-factor authentication on all systems that hold or access client information. Phishing-resistant authentication methods used where supported.
Endpoint Platform	All endpoints used to access, process, or store client information are hardened against an internal baseline derived from recognized industry benchmarks. Specific platform details are withheld from this Policy as a matter of operational security and are available under NDA on request.
Personnel	Single principal (Brian Hahn). No employees with access to client information. Any subcontractor is bound by written confidentiality and security obligations no less protective than this Policy.

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

Background Screening	Principal: financial services and Wall Street trading background; 300+ cyber and IT audits conducted in financial sector. Any future personnel subject to documented background screening appropriate to the role.
Information Security Program	Documented in this Policy. Defense-in-depth, compartmentalized architecture, least-privilege access, encrypted storage and transit, logging and monitoring.
Risk Assessments and Threat Detection	MTradecraft performs documented internal risk assessments and threat detection processes on its own systems on an ongoing basis, including recurring external vulnerability scans of its own internet-facing infrastructure with the same tooling used in client CRVT engagements, and applies the same methodology in its CRVT assessments for client engagements.
Material Nonpublic Information (MNPI)	MNPI encountered during an engagement is safeguarded as Client Information under this Policy. MTradecraft does not trade on, or communicate to others, MNPI obtained through an engagement, consistent with Exchange Act Section 10(b) and Rule 10b-5. See Section 3.5.
Incident Response Plan	Documented in Section 5. Written, tested annually, with defined phases, notification timing, and recordkeeping.
Breach Notification to Client	As soon as possible, and in no event later than 72 hours after becoming aware that a breach in security has occurred involving unauthorized access to or use of client information — satisfying the Regulation S-P § 248.30(a)(5)(i)(B) service provider standard.
Subcontractor / Fourth Party Use	MTradecraft does not currently subcontract client-facing work or share client information with subcontractors. Any future subcontractor will be subject to advance written notice and contractual flow-down of these obligations.
Cloud Services Used	No general-purpose consumer cloud productivity suites are used for client information. Limited use of self-hosted infrastructure for tooling and CRM, under MTradecraft's control.
AI and LLM Use	Any AI or large language model work involving client information is performed using local AI models running on MTradecraft-controlled, hardened infrastructure with no transmission of client data to external AI services or model providers. Client information is not used to train any third-party model. Cloud-based AI services are limited to non-client research and administrative tasks. AI use is governed against the SANS Critical AI Security Controls and mapped to Rule 206(4)-7 expectations. See Section 4.5 of this Policy.
Client Security Training Requirements	Upon request, MTradecraft personnel will review and acknowledge a client's security policies and complete client-provided security awareness training materials as part of engagement onboarding.
Data Retention	Client work product retained for the duration of the engagement plus five (5) years to satisfy recordkeeping expectations. Earlier deletion available upon written client request, subject to legal hold.
Data Destruction	Cryptographic erasure or multi-pass overwrite of electronic media; physical destruction of end-of-life storage; cross-cut shred of paper. Disposal is logged.
Insurance	Cyber liability and professional liability (errors & omissions) coverage in place. Certificates of insurance available to clients on request.
Business Continuity / Disaster Recovery	Encrypted offline backups; documented recovery procedures for key tools, evidence stores, and CRM. Single-principal continuity contingency documented for client notification in the event of principal incapacity. No material business or service disruption has occurred in the twelve (12) months preceding the effective date of this version.
Independence	MTradecraft does not resell hardware, MSP services, or third-party products. Receives no vendor commissions or referral fees. Recommendations are vendor-independent.
Right to Audit	Clients may, on reasonable written notice, request evidence of compliance with this Policy, including SOC-equivalent self-attestations, screenshots of control state, and incident records pertaining to that client's data.
Regulatory Examinations and Litigation	MTradecraft has not been the subject of any regulatory enforcement action, material litigation, or reportable cybersecurity incident.

MTradecraft, LLC
Dallas, TX
210-201-2102
info@mtradecraft.com

Privacy Notice	MTradecraft does not engage in joint marketing or third-party data sharing requiring a Regulation S-P opt-out. This Policy serves as MTradecraft's privacy disclosure to clients.
Policy Review Cadence	At least annually and after any material change or reportable incident.

9. Acknowledgment

By engaging MTradecraft, LLC, the client acknowledges receipt of this Privacy, Information Security, and Incident Response Policy. MTradecraft acknowledges and accepts its obligations as a service provider to a covered institution under SEC Regulation S-P, including the seventy-two (72) hour breach notification commitment set forth in Section 5.2.

MTradecraft, LLC
Dallas / McKinney, Texas
210-201-2102
info@mtradecraft.com
https://mtradecraft.com