TZERO LABS

Oil & Gas Testing | Inspection Coordination | Petroleum Product Verification

Data Ethics, Privacy & Information Security Framework

Governing Inspection Data Integrity and Client Confidentiality

Document Reference	SEC-FRM-001
Version	1.0
Effective Date	January 2025
Classification	Confidential — Internal Use
Jurisdiction	United States of America

TZERO LABS

Data Ethics, Privacy & Information Security Framework

Document Reference: SEC-FRM-001 | Version 1.0 | 2025

Standards Alignment: ISO 27001 | NIST CSF | GDPR | SOC 2 | US State Privacy Laws

CLASSIFICATION	VERSION	PREPARED BY	DISTRIBUTION
TOP CONFIDENTIAL	1.0 — 2025	CISO & Compliance Office	Auditors · Regulators · Clients

Framework Scope

This Framework governs data ethics principles, privacy operations, information security controls, incident response, and continuous compliance monitoring across all Tzero Labs systems, operational platforms, and client-facing data environments.

"The integrity of our data is the integrity of our service."

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

Tzero Labs' Data Ethics, Privacy & Information Security Framework ("the Framework") establishes the governing principles, policies, technical controls, and accountability structures required to protect all personal data, confidential operational information, client cargo data, laboratory test results, inspection documentation, and technology assets across the organisation.

As a United States-based oil and gas testing, inspection coordination, dip testing, and petroleum product verification company, Tzero Labs handles data that is operationally and commercially sensitive to a wide range of clients — including buyers, sellers, petroleum traders, refineries, tank farms, terminal operators, and shipping companies. The accuracy, confidentiality, and integrity of inspection reports, certificate of quality data, dip test records, sampling documentation, and cargo quantity verification files are fundamental to the trust clients place in Tzero Labs and to the legitimate completion of petroleum transactions.

This Framework is aligned with ISO/IEC 27001:2022, the NIST Cybersecurity Framework (CSF) 2.0, GDPR, applicable US state data privacy laws, and SOC 2 Type II requirements. It applies to all Tzero Labs employees, contractors, field inspection coordinators, laboratory liaisons, and third-party service providers. It is reviewed annually by the Compliance Council and independently audited in accordance with ISO 27001 certification requirements.

02 DATA ETHICS PRINCIPLES

Tzero Labs is committed to the ethical collection, use, and stewardship of all data — including inspection reports, petroleum product test results, client transaction records, cargo quantity data, and laboratory findings. Our data ethics principles extend beyond legal compliance. They reflect our responsibility to clients who depend on the accuracy and confidentiality of every piece of data we handle in order to conduct safe, credible, and compliant petroleum transactions.

PRINCIPLE	COMMITMENT
LAWFULNESS	All data processing has a documented, valid legal basis. Inspection data, cargo records, and petroleum test results are processed only under valid contractual authority or with appropriate client authorisation.
FAIRNESS & TRANSPARENCY	Clients and data subjects are informed about how their data is used. Inspection results and laboratory findings are communicated only through authorised channels and to authorised parties. No hidden processing of client transaction data.
PURPOSE LIMITATION	Data — including petroleum product specifications, cargo quantities, sampling results, and certificate of quality information — is collected for specified, legitimate purposes and is not used for any other commercial, analytical, or operational purpose without explicit authorisation.
DATA MINIMISATION	Only data that is adequate, relevant, and necessary for the stated inspection, verification, or coordination purpose is collected and retained.

ACCURACY	Inspection reports, certificate of quality data, dip test records, and laboratory test results are verified for accuracy before transmission. Errors are identified and corrected promptly.
STORAGE LIMITATION	Data is retained only for as long as required for the operational or contractual purpose, or by applicable legal obligation. Retention periods are governed by the Tzero Labs Retention Schedule (Form DPR-SCH-001).
INTEGRITY & CONFIDENTIALITY	Technical and organisational measures protect all inspection data, client information, and laboratory records against unauthorised access, accidental loss, tampering, or disclosure.
ACCOUNTABILITY	Tzero Labs takes full responsibility for demonstrating compliance with all applicable data protection obligations and for the responsible stewardship of all client and operational data entrusted to us.

03 PRIVACY GOVERNANCE STRUCTURE

Privacy governance at Tzero Labs operates through a three-tier structure: Board-level oversight, a cross-functional Compliance Council, and specialist operational roles. This structure ensures that data protection and information security obligations are embedded throughout the organisation — from corporate operations to field inspection coordination and laboratory liaison functions.

Governance Structure:

Board of Directors (Data Governance Oversight) → Compliance Council (DPO, CISO, Legal) → Data Protection Officer / CISO / Information Security Team

Quarterly Privacy & Security Reviews → Annual Independent Audit → Regulator Reporting as Required

3.1 Key Roles & Responsibilities

Role	Appointed By	Key Responsibilities	Reporting Line
Data Protection Officer (DPO)	Board / CEO	Privacy compliance, data subject rights, regulatory liaison, staff guidance	Compliance Council → Board
Chief Information Security Officer (CISO)	CEO	ISO 27001, security architecture, incident management	Compliance Council → CEO
Information Security Lead	CISO	System controls, data mapping, access management, Privacy by Design	CISO / DPO
Data Owners (per	Functional Heads	Classification, access	Respective Department

system/domain)		decisions, retention management	Heads
Information Security Analysts	CISO	Monitoring, vulnerability management, incident response	CISO

04 DATA CLASSIFICATION FRAMEWORK

All data assets held or processed by Tzero Labs must be classified according to the four-tier classification scheme below. Given the commercially sensitive nature of petroleum inspection, cargo verification, and transaction support data, Tzero Labs applies strict handling controls at all classification levels. Data Owners are responsible for classifying data assets under their accountability.

TOP SECRET / RESTRICTED

Highest sensitivity — C-suite & board only

Examples: Unreleased client transaction data, proprietary pricing arrangements, strategic commercial information

CONFIDENTIAL

Sensitive business & client data — need-to-know

Examples: Client inspection reports, certificates of quality, dip test records, cargo quantities, sampling findings, client identities on active petroleum transactions, petroleum product specifications

INTERNAL USE ONLY

Internal operational data — all staff

Examples: Internal procedures, operational checklists, approved vendor lists, scheduling records, staff directories

PUBLIC

Approved external communications only

Examples: Company overview, published policy documents, public service descriptions

Data Classification Levels — Highest to Lowest Sensitivity

05 DATA OWNERSHIP & ACCOUNTABILITY

Every data asset within Tzero Labs must have a designated Data Owner, Data Custodian, and Data Processor. These roles carry distinct accountability for the data lifecycle from collection through disposal. In the context of petroleum inspection and cargo verification, the chain of custody for data is as important as the chain of custody for physical samples.

Role	Accountability	Examples
Data Controller (TZL)	Legal entity responsible for purpose and means of processing	Tzero Labs as organisation — bound by applicable privacy law
Data Owner	Business accountable for a data domain; approves access; sets	Operations Director owns inspection records; Finance Director

	classification	owns financial records
Data Custodian	Technical steward; implements controls defined by the Data Owner	IT Operations, System Administrators
Data Processor	Third party processing data on behalf of Tzero Labs under contract	Accredited laboratories, cloud service providers, reporting platforms
Data Subject	Individual whose personal data is processed; holds applicable privacy rights	Employees, field personnel, client contacts, inspection witnesses

06 ACCESS CONTROL POLICY

Tzero Labs implements a Role-Based Access Control (RBAC) model enforced through a Zero Trust security architecture. Access to all systems, data, and operational records — including inspection reports, laboratory findings, dip test data, and client cargo verification files — is granted on the principle of Least Privilege. Users receive the minimum permissions necessary to perform their role. Access rights are reviewed quarterly.

6.1 Zero Trust Architecture Principles

- Never trust, always verify — no implicit trust based on network location or user identity
- Verify explicitly — authenticate and authorise every access request based on all available data points
- Use least privilege access — limit user access with just-in-time (JIT) and just-enough-access (JEA) principles
- Assume breach — minimise blast radius; segment access; verify end-to-end encryption; employ continuous analytics
- Continuously validate — session re-verification on anomalous behaviour or privilege escalation attempts

07 IDENTITY & ACCESS MANAGEMENT

Tzero Labs' Identity and Access Management (IAM) platform provides centralised authentication, authorisation, and lifecycle management for all user identities — including employees, field inspection coordinators, laboratory liaisons, contractors, and privileged administrators.

Control	Standard	Implementation	Status
Single Sign-On (SSO)	SAML 2.0 / OAuth 2.0 / OIDC	Centralised identity provider for all applications	DEPLOYED
Privileged Access Management (PAM)	HashiCorp Vault	Vaulted credentials; session recording for privileged users	DEPLOYED
User Lifecycle Management	ISO 27001 A.9	Automated joiner/mover/leaver workflows	DEPLOYED
Access Review Cadence	ISO 27001 A.9.2.5	Quarterly automated access certification	ACTIVE

		reviews	
Service Account Management	NIST SP 800-63	Dedicated accounts; no shared credentials	ENFORCED
Directory Services	LDAP / Active Directory	Federated identity; group-based provisioning	DEPLOYED

08 MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication (MFA) is mandatory for all user accounts accessing Tzero Labs systems — including the inspection management platform, laboratory reporting portal, client documentation systems, and all internal operational databases. MFA requirements are enforced at the identity provider level and cannot be disabled by individual users. Exemptions require CISO written approval and compensating control documentation.

System / Access Type	MFA Method Required	Enforcement
Corporate Email & Productivity	TOTP App (Authenticator) or Hardware Key	MANDATORY — No bypass permitted
Cloud Infrastructure	Hardware Security Key (FIDO2/YubiKey) + PIN	MANDATORY — All privileged accounts
VPN / Remote Access	Certificate + TOTP or Push Notification	MANDATORY — All remote sessions
Inspection Management Platform (non-SSO)	TOTP + SMS as fallback (deprecating 2026)	MANDATORY
Privileged Admin Accounts	Hardware Key + PAM session recording	MANDATORY — Step-up auth required
Field Coordinator / Third-Party Access	TOTP + Session time-limited token	MANDATORY — Time-boxed access only
Client-Facing Portals	TOTP or Passkey (FIDO2)	MANDATORY for document-accessing users

09 ENCRYPTION STANDARDS

Tzero Labs applies defence-in-depth encryption across all data states. This is particularly critical given the commercially sensitive nature of petroleum inspection data, cargo verification results, certificate of quality records, and client transaction information — which, if intercepted or tampered with, could have significant financial and reputational consequences for our clients. Cryptographic standards are reviewed annually against NIST guidance.

Data State	Standard	Key Management	Status
Data at Rest — Databases	AES-256-GCM	AWS KMS / Azure Key Vault (HSM-backed)	ENFORCED

Data at Rest — File Storage	AES-256-CBC	Envelope encryption; key rotation every 90 days	ENFORCED
Data in Transit — External	TLS 1.3 (TLS 1.2 minimum)	Certificate pinning; HSTS enforced	ENFORCED
Data in Transit — Internal	mTLS 1.3	Zero-trust internal service mesh	ENFORCED
Backups	AES-256 + separate backup key	Offsite key escrow; WORM storage	ENFORCED
Email (Sensitive / Inspection Reports)	S/MIME or PGP	Cert-based; auto-encrypt on classification tag	DEPLOYED
Mobile Devices	Device-level AES-256 (MDM enforced)	MDM key management; remote wipe enabled	ENFORCED
Passwords & Secrets	Argon2id (hashing); vault-stored secrets	HashiCorp Vault; no plaintext secrets permitted	ENFORCED

All data flows are encrypted in transit (TLS 1.3) and at rest (AES-256)

10 DATA RETENTION POLICY

Data shall not be retained beyond the period necessary for the specified operational purpose or applicable legal requirement. Petroleum inspection records, laboratory test results, dip test documentation, and cargo verification files are subject to minimum retention periods aligned with both industry practice and client contractual requirements. The Tzero Labs Retention Schedule (Form DPR-SCH-001) is the authoritative reference for all retention periods.

Data Category	Retention Period	Legal Basis	Disposal Method
Inspection Reports & Certificate of Quality Data	Contract term + 7 years	Contractual / regulatory obligation	Secure deletion + certificate
Dip Test Records & Sampling Documentation	7 years minimum	Industry standard / client contractual requirements	Secure archive → deletion
Client Cargo & Transaction Records	Contract term + 5 years	Contractual obligation	Automated purge + audit log
Employee Personal Data (active)	Duration of employment + 7 years	Employment law / tax compliance	Secure deletion + certificate
Financial Records	7 years	Tax & company law obligations	Secure shred + digital deletion
Security Logs & SIEM Data	12 months (hot) + 24 months (cold)	ISO 27001; incident investigation	Encrypted archive → deletion
Contract Data	Contract term + 10 years	Legal obligation;	Secure archive → deletion

		limitation periods	
Marketing Data (consented)	Until withdrawal + 30 days	Consent-based processing	Automated erasure on withdrawal

11 DATA DISPOSAL PROCEDURES

All data disposal must be carried out in accordance with the classification level of the data. Given the commercial sensitivity of petroleum inspection, cargo verification, and client transaction records, disposal of Confidential and Top Secret / Restricted data requires verified and witnessed procedures. Proof of disposal must be retained for 3 years.

Classification	Digital Disposal	Physical Disposal	Verification
Top Secret / Restricted	DoD 5220.22-M (7-pass overwrite) or crypto-erasure	Cross-cut shred (DIN 66399 P-5 min); witnessed	Written certificate; witness signature
Confidential	3-pass overwrite or crypto-erasure	Cross-cut shred (DIN 66399 P-4)	Certificate of destruction
Internal Use Only	Single-pass overwrite or secure delete tool	Standard cross-cut shred	Automated deletion log
Public	Standard delete + empty recycle bin	Standard recycling	No additional verification required

12 PRIVACY PROTECTION CONTROLS

Tzero Labs implements Privacy by Design and by Default across all systems and processes involving personal data or commercially sensitive operational information. Privacy impact is assessed before any new processing activity, system implementation, or client platform deployment begins. The following technical and organisational measures (TOMs) are in force.

Control	Implementation
Data Minimisation	Collect only what is strictly necessary for the inspection, verification, or coordination activity; automated field-level minimisation checks in data pipelines
Pseudonymisation	Personal identifiers replaced with tokens in analytics, development, testing, and reporting environments
Privacy Impact Assessments (DPIAs)	Mandatory for all high-risk processing activities; DPO sign-off required before implementation
Consent Management	Granular consent captured and stored; withdrawal honoured within 30 days; audit trail maintained throughout

Data Subject Rights	Access, erasure, portability, restriction, objection — all requests fulfilled within applicable legal timescales
Third-Party Data Processing	Data Processing Agreement in place with all third-party processors, including accredited laboratories, inspection coordination platforms, and cloud service providers
Records of Processing Activities	ROPA maintained and reviewed quarterly; complete for all processing activities
Privacy Notices	Clear, plain-language notices for all data collection touchpoints; reviewed and updated annually

13 INCIDENT RESPONSE FRAMEWORK

Tzero Labs maintains a documented, tested Incident Response Plan (Form SEC-IRP-001) aligned with NIST SP 800-61 Rev. 2 and ISO/IEC 27035. The plan covers security events affecting any system that holds or processes inspection data, laboratory results, client cargo information, certificate of quality records, or corporate operational data. The plan is tested via annual tabletop exercises and bi-annual simulated incident drills.

NIST Cybersecurity Framework — Core Functions Applied at Tzero Labs:

- **IDENTIFY** — Asset management, risk assessment, governance, inspection data inventory
- **PROTECT** — Access control, encryption, security awareness training, inspection data confidentiality protocols
- **DETECT** — Continuous monitoring, anomaly detection, SIEM correlation
- **RESPOND** — Incident response, communications, analysis, client notification protocols
- **RECOVER** — Recovery planning, improvements, post-incident reporting

Incident Response Decision Flowchart:

Security Incident Detected → Initial Triage & Severity Assessment → Critical or High Severity? → YES: Activate IRT / Notify DPO + CISO within 1 Hour → Containment & Eradication → Post-Incident Review & Lessons Learned | NO: Log & Monitor (Low Severity) → Evidence Preservation

14 BREACH NOTIFICATION PROCEDURES

In the event of a personal data breach or an unauthorised disclosure of confidential inspection, cargo, or client transaction data, Tzero Labs is required to comply with mandatory notification obligations under applicable US state privacy laws and, where applicable, GDPR (Articles 33/34). Particular attention is given to breaches involving petroleum transaction data, certificate of quality records, and client cargo information given the potential for significant commercial harm.

Breach Notification Timeline:

0H (Breach Detected) → 1H (IRT Activated) → 4H (DPO Notified) → 24H (Internal Escalation) → 48H (Risk Assessment) → 72H (Regulatory Notification where required) → 7D (Data Subject Notification) → 30D (Post-Incident Report)

Trigger Condition	Action Required	Responsible	Timeline

Any suspected breach identified	Log in Incident Register; notify IRT & DPO	Discovering employee / IT	Immediately — within 1 hour
Breach confirmed — low risk to individuals	Internal report; remediation; no external notification required	DPO + CISO	Within 24 hours
Breach confirmed — risk to individuals	Notify supervisory authority where required	DPO	Within 72 hours of discovery
High risk to rights & freedoms	Notify affected data subjects directly	DPO + Communications	Without undue delay after regulator
Third-party processor breach	Processor notifies Tzero Labs; TZL then follows above process	Processor within 24h; TZL DPO	Per processor contract
Post-incident	Root cause analysis; lessons learned; control update	CISO + DPO	Within 30 days of closure

15 SECURITY AWARENESS PROGRAM

The Tzero Labs Security Awareness & Training Program is mandatory for all employees, contractors, field inspection coordinators, and third-party users with access to Tzero Labs systems. Training is risk-based, role-differentiated, and continuously updated to reflect the current threat landscape — including phishing risks targeting petroleum trading data, social engineering attempts directed at inspection personnel, and physical security threats at port and terminal environments.

Training Module	Target Audience	Frequency	Format	Completion Rate
Security Foundations	All staff + contractors	Annual + on-boarding	eLearning + assessment	100%
Phishing Awareness & Simulation	All staff	Quarterly simulation; annual training	Simulated attacks + debrief	100%
Data Protection & Privacy	All staff handling client or inspection data	Annual	eLearning + quiz	100%
Privileged Access & PAM	IT Admin / Privileged users	Annual + on change	Instructor-led workshop	100%
Incident Reporting Procedure	All staff	Annual	Micro-learning	100%
Inspection Data Confidentiality & Chain of Custody	Field coordinators, laboratory liaisons, inspection personnel	Annual	Scenario-based training	100%

Executive Cyber Briefing	Board + C-suite	Semi-annual	Facilitated briefing	100%
Social Engineering & Physical Security	All staff	Annual	Scenario-based eLearning	99%

16 CONTINUOUS MONITORING

Tzero Labs operates a 24/7 Security Operations function with automated threat detection, SIEM correlation, and real-time alerting. The monitoring programme is aligned with the NIST SP 800-137 continuous monitoring framework and CIS Controls v8.

Monitoring Layer	Tool / Technology	Coverage	Alert Response SLA
SIEM — Log Aggregation	Splunk / Microsoft Sentinel	All systems, applications, network	Critical: 15 min; High: 1 hr
Endpoint Detection & Response	CrowdStrike Falcon / Defender ATP	100% managed endpoints	Critical: 15 min real-time
Network Traffic Analysis	Darktrace / Zeek IDS	All network segments + cloud environments	Anomaly alert: 30 min
Vulnerability Management	Tenable Nessus / Qualys	Weekly scan; critical assets daily	Critical CVE patch: 24 hours
Cloud Security Posture Management	AWS Security Hub / Prisma Cloud	All cloud environments	Misconfiguration: 4 hours
Data Loss Prevention (DLP)	Microsoft Purview / Symantec DLP	Email, endpoint, cloud storage	Policy violation: real-time block
Dark Web & Threat Intelligence	Recorded Future	Credential and data exposure monitoring	Credential exposure: 1 hour
Penetration Testing	External certified provider	Annual full test; quarterly targeted	Remediate Critical: 30 days

17 COMPLIANCE & AUDIT REQUIREMENTS

Tzero Labs' Information Security and Privacy compliance programme is aligned to a multi-framework approach. Compliance status is assessed internally on a quarterly basis and independently audited annually.

17.1 Audit Schedule

Audit Type	Scope	Frequency	Conducted By
ISO 27001 Surveillance	ISMS controls & effectiveness	Annual	Accredited certification body
ISO 27001 Recertification	Full ISMS re-certification	Every 3 years	Accredited certification body

SOC 2 Type II	Security, Availability, Confidentiality	Annual	Licensed CPA firm
Privacy Impact Assessment Review	High-risk processing activities	Annual + on new processing	DPO + Internal Audit
Penetration Test	External & internal; web apps & API	Annual (full); quarterly (targeted)	Certified external provider
Internal ISMS Audit	All ISO 27001 controls	Semi-annual	Internal Audit / CISO
Supplier Security Audit	Critical third-party processors including accredited laboratories	Annual or on contract renewal	Security team

18 APPROVAL & DOCUMENT CONTROL

This Framework has been reviewed and approved by the Tzero Labs Compliance Council and Board of Directors. It supersedes all previous information security and privacy policy documents.

DOCUMENT APPROVAL SIGNATURES

Role	Name	Signature	Date
Chief Information Security Officer	_____	_____	_____
Data Protection Officer	_____	_____	_____
CEO / Managing Director	_____	_____	_____

Document Title	Data Ethics, Privacy & Information Security Framework
Document Reference	SEC-FRM-001
Version	1.0 — Effective January 1, 2025
Framework Alignment	ISO 27001:2022, NIST CSF 2.0, GDPR, US State Privacy Laws, SOC 2, CIS Controls v8
Prepared By	Tzero Labs CISO & Compliance Office
Approved By	Compliance Council & Board of Directors
Review Frequency	Annual or following material security event / regulatory change
Next Review Date	January 2026
Distribution	Employees · Clients · Auditors · Regulators (on request)