

Anti Money Laundering Counter Terrorist Financing and Proliferation Financing Policy

Hamilton Energi Ltd | United Kingdom | Version 1.0

1. Purpose and policy statement

Hamilton Energi Ltd is committed to preventing its business, people, products, services and supply chain from being used to launder criminal property, finance terrorism, evade sanctions or finance the proliferation of weapons of mass destruction. We will take a proportionate, risk-based approach, cooperate with competent authorities and never knowingly facilitate financial crime.

2. Legal and regulatory framework

This policy supports compliance, where applicable, with the Proceeds of Crime Act 2002, the Terrorism Act 2000, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended, the Sanctions and Anti-Money Laundering Act 2018, applicable UK financial sanctions regulations, and guidance issued by the Company's supervisory authority and the UK Financial Intelligence Unit. The Company will identify which requirements apply to its business and obtain specialist legal or regulatory advice where necessary.

3. Scope

This policy applies to all directors, officers, employees, temporary workers, contractors and agents of Hamilton Energi Ltd, and to all UK operations and controlled entities. Joint ventures and other associated businesses should adopt equivalent controls. Compliance with this policy is a condition of engagement. Local procedures may impose stricter requirements but must not weaken this policy.

4. Key definitions

- **Money laundering:** concealing, converting, transferring, acquiring, using or possessing criminal property, or facilitating those acts.
- **Terrorist financing:** providing, collecting or using funds or property for terrorist purposes.
- **Proliferation financing:** providing funds or financial services connected with the manufacture, acquisition, possession, development, movement or use of chemical, biological, radiological or nuclear weapons and related materials or technology.
- **Beneficial owner:** the natural person who ultimately owns or controls a customer or on whose behalf a transaction is conducted.
- **Customer due diligence (CDD):** identifying and verifying a customer and beneficial owner, understanding the purpose and intended nature of the relationship, and conducting ongoing monitoring.

- **Politically exposed person (PEP):** a person entrusted with a prominent public function, including relevant family members and known close associates, as defined by applicable law.
- **Suspicion:** a genuine possibility, based on available facts, that is more than fanciful; proof is not required.

5. Governance and responsibilities

- Paul Hamilton, Director: approves this policy, sets risk appetite and receives proportionate management information.
- **Senior management:** ensures adequate resources, effective controls and prompt remediation.
- Officer responsible for compliance: Paul Hamilton, Director oversees compliance with applicable regulations and reports to senior management.
- Nominated Officer/Money Laundering Reporting Officer (MLRO): Paul Hamilton, Director, customers@hamiltonenergi.com receives internal disclosures, assesses whether a Suspicious Activity Report (SAR) is required, seeks a defence against money laundering where appropriate, maintains confidential records and liaises with the National Crime Agency and supervisory authority.
- **Managers:** embed controls in their areas and escalate concerns.
- **All personnel:** complete training, follow procedures, remain alert and report concerns immediately. No person may investigate a suspicion independently or disclose that a report has been made where this could prejudice an investigation.

6. Business-wide risk assessment

The Company will maintain a documented assessment of its exposure to money laundering, terrorist financing and proliferation financing. It will consider customers and beneficial owners; countries and geographic links; products and services; transactions and payment methods; delivery channels; intermediaries; new technologies; sanctions exposure; and information from national, sector and supervisory risk assessments. Controls will be proportionate to recorded risk ratings. The assessment will be approved by senior management and reviewed at least annually and when material changes or incidents occur.

7. Customer and third-party due diligence

- Complete proportionate due diligence before establishing a relationship or carrying out a transaction where required by law or Company procedure.
- Identify and verify the customer, beneficial owner and any person acting on the customer's behalf using reliable, independent information.
- Understand ownership and control, the nature and purpose of the relationship, expected activity, source of funds and, where risk requires, source of wealth.
- Screen relevant parties against applicable UK sanctions lists and assess PEP and adverse-information risk using approved systems.
- Keep due diligence current and monitor transactions and behaviour against the expected profile.

- Do not start or continue a relationship, release funds or complete a transaction if required due diligence cannot be completed. Escalate promptly to the MLRO and follow their direction.

7.1 Enhanced and simplified due diligence

Enhanced due diligence (EDD) and enhanced ongoing monitoring must be applied where required by law or where higher risk is identified, including relevant PEP relationships, high-risk jurisdictions, complex or unusually large transactions, opaque ownership, unexplained third-party payments or other circumstances presenting elevated risk. EDD may include additional verification, senior-management approval, corroboration of source of funds or wealth, and more frequent review. Simplified due diligence may be used only where legally permitted, a documented low risk exists and no suspicion or other mandatory EDD trigger is present.

8. Warning signs

- Unusual secrecy, reluctance or inconsistent identity or ownership information.
- Transactions without an apparent commercial purpose, or inconsistent with the customer's profile.
- Complex structures, rapid movement of funds, multiple accounts or unnecessary intermediaries.
- Cash, overpayments, refunds to a different account, unexplained third-party payments or payments split to avoid controls.
- Links to sanctioned persons, high-risk jurisdictions, shell companies, nominee arrangements or adverse information.
- Pressure to bypass controls, unusual urgency, false documents or abrupt changes in instructions.
- Goods, technology, counterparties or routes associated with sanctions evasion or proliferation risk.

9. Reporting suspicions

1. Any person who knows or suspects, or has reasonable grounds to know or suspect, money laundering or terrorist financing must report the matter immediately and confidentially to the MLRO using customers@hamiltonenergi.com, addressed to Paul Hamilton, Director.
2. The report must state the persons involved, relevant dates, transactions, amounts, accounts, supporting facts, the reason for suspicion and any imminent deadline. Do not delay because information is incomplete.
3. The MLRO will assess the disclosure, document the decision and submit a SAR to the UK Financial Intelligence Unit through the approved NCA reporting route where required.
4. If proceeding could involve dealing with criminal property, the MLRO will determine whether a defence against money laundering is required and whether activity must be paused. Personnel must not proceed unless authorised.
5. Reports and related information are strictly confidential. Personnel must not "tip off" a subject or otherwise prejudice an investigation. Questions must be directed only to the MLRO or authorised legal adviser.
6. A SAR does not replace reporting a crime, fraud, sanctions breach or other matter through the appropriate separate channel.

10. Transaction, payment and sanctions controls

- Use approved bank accounts and payment methods; cash transactions are prohibited unless expressly authorised under a documented procedure.
- Apply segregation of duties and appropriate approval thresholds to customer, supplier, refund and bank-detail changes.
- Verify changes to payment instructions independently using trusted contact details.
- Do not make or receive payments for unrelated third parties without documented rationale and approval.
- Screen relevant parties and transactions at onboarding, periodically and when ownership, control, geography or sanctions information changes.
- Freeze, reject, hold or escalate activity only in accordance with applicable law and instructions from the MLRO, sanctions lead or legal counsel.

11. Training, screening and awareness

Relevant personnel will receive risk-based training at induction and periodically thereafter, with enhanced training for higher-risk roles and the MLRO. Training will cover legal duties, red flags, due diligence, sanctions, internal reporting, confidentiality, tipping off and practical scenarios. Completion and understanding will be recorded. Where appropriate to the size and nature of the business, relevant employees will be screened before appointment and during employment for competence, conduct and integrity.

12. Records and data protection

The Company will retain risk assessments, due diligence and verification evidence, transaction and monitoring records, approvals, training records, internal disclosures, SAR decisions and control testing in a secure and retrievable form. Where the 2017 Regulations apply, CDD and transaction records will normally be retained for five years after the end of the business relationship or completion of an occasional transaction, then securely deleted unless a lawful exception applies. Other records will follow the Company retention schedule and applicable law. Access will be limited to authorised persons, and personal data will be processed in accordance with UK data protection law.

13. Monitoring, assurance and breaches

The Company will test the design and operation of AML controls according to risk. Management information may include due diligence completion, high-risk relationships, screening alerts, internal disclosures, training, overdue reviews and remediation. Where appropriate, an independent audit function will assess effectiveness and track recommendations. Actual or suspected breaches must be reported immediately to the MLRO and Paul Hamilton, Director. The Company will investigate appropriately, preserve evidence, remediate control failures and make regulatory, law-enforcement or sanctions reports where required. Retaliation against a person who raises a concern in good faith is prohibited. Breaches may result in disciplinary action, termination of engagement and referral to authorities.

14. Policy review and approval

This policy will be reviewed at least annually and sooner following legal or regulatory change, material changes to the business or its risk exposure, control failures, enforcement findings or significant incidents. Material amendments require approval by Paul Hamilton, Director.

15. Contacts and document approval

MLRO/Nominated Officer	Paul Hamilton, Director customers@hamiltonenergi.com
Deputy/alternate	External legal or compliance adviser arranged by Paul Hamilton, Director, when required
Internal reporting channel	customers@hamiltonenergi.com Address confidential reports to Paul Hamilton, Director
Policy owner	Paul Hamilton, Director
Approved by	Paul Hamilton, Director
Approval date	30 September 2026
Next review date	30 September 2027