DUE DILIGENCE AND TRADE COMPLIANCE POLICY

TRIO Integration Information Technologies Education Trade Inc.

1) Purpose and Scope

This policy has been established to define the due diligence and trade compliance rules to be applied in all business relationships conducted by TRIO with distributors, resellers, sub-distributors, suppliers, and third parties.

The main objective of the policy is to confirm the reliability of third parties in terms of identity, ownership, reputation, and transparency, to prevent risks of bribery and corruption, and to ensure full compliance with national and international trade legislation.

TRIO undertakes to fulfill its legal obligations by reviewing all business partners in compliance with U.S. export control and sanctions laws (EAR and OFAC (https://sanctionssearch.ofac.treas.gov)), the FCPA, local legislation, and the provisions of the Dell EMC Partner Code of Conduct.

2) Basic Principles

In line with the principle of compliance, TRIO requires adherence to the U.S. Export Administration Regulations (EAR), OFAC sanctions (https://sanctionssearch.ofac.treas.gov), the Foreign Corrupt Practices Act (FCPA), the Transparency International CPI, and local legislation. By adopting a risk-based approach, it evaluates all third-party relationships according to their risk levels. While basic identity verification is sufficient for low risk, PEP checks and license assessments are mandatory for high-risk cases.

In accordance with the principle of transparency, all business partners are obliged to provide the necessary information completely and accurately. Providing false, incomplete, or misleading information is considered a serious violation and may result in the suspension of the business relationship.

A zero-tolerance principle applies to all business processes. Bribery, corruption, export violations, sanctions violations, and unethical conduct are under no circumstances permitted. Such violations must be reported immediately to the Ethics & Compliance team.

2.1 New Customer Onboarding (ABC & Sanctions Compliance Vetting)

Before any first transaction, TRIO performs an Anti-Bribery & Corruption (ABC) and trade-sanctions compliance review. The steps below must be completed in full. Findings are documented and, where warranted, escalated to Legal and the Ethics & Compliance function.

a. KYC & Document Collection

Collect core KYC data: registered legal name, registration/VAT numbers, address, line of business, contact details, and authorized signatories.

b. UBO (Ultimate Beneficial Owner) Identification

Map the ownership structure to the ultimate natural-person owners. Flag opaque or unusually complex structures as red flags and escalate as needed.

c. PEP Screening

Assess the customer, its directors/officers, and UBOs against the FATF definition of Politically Exposed Person (PEP) (*https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html*).
Apply Enhanced Due Diligence (EDD) if a PEP link is identified.

d. Sanctions & Restricted-Party Screening

Search names (including common transliterations and address variants) across the following official sources. Keep screenshots/exports of the exact queries and results.

- U.S. Treasury – OFAC Sanctions List Search (*https://sanctionssearch.ofac.treas.gov/*)
- U.S. Government – Consolidated Screening List (CSL) (*https://www.trade.gov/data-visualization/csl-search*)
- European Union – EU Sanctions Map / Consolidated Lists (*https://www.sanctionsmap.eu/*)
- United Kingdom – Consolidated Sanctions List Search (OFSI) (*https://search-uk-sanctions-list.service.gov.uk/*)
- United Nations – Security Council Consolidated List (*https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list*)

e. Adverse Media & Legal/Regulatory Checks

Search reputable media and public court/official notices for fraud, bribery, corruption, sanctions evasion, money laundering, export-control violations, or similar concerns. Capture evidence of sources and dates.

f. Risk Scoring & Approvals

Assign a risk score considering country risk, sector/use-case, end-use/end-user, supply-chain routing, and payment method. Medium/high-risk applications require management approval prior to onboarding.

g. Recordkeeping

Retain all screening artifacts (search strings, timestamps, screenshots/exports, decisions, and approvals) for at least five (5) years or longer where required by law.

h. Decline/Escalation Triggers

Decline and escalate where there is a confirmed sanctions listing, unverifiable UBOs, unexplained end-use/end-user, suspicious transshipment routes, or close PEP ties without satisfactory risk mitigation.

i. Re-Screening Triggers After Onboarding

Re-screen upon changes to legal name, ownership/UBO, geography, products/end-use, or upon credible negative-news signals.

2.2 Periodic Screening of Existing Customers (Quarterly Sanctions Screening)

TRIO conducts quarterly sanctions and restricted-party screening for all existing customers. This control is independent of new-customer onboarding and is performed as a recurring safeguard under the principles below:

1. **Scope**
   All active customers-legal entities and natural persons-including parent entities, subsidiaries/affiliates, directors/officers, and Ultimate Beneficial Owners (UBOs).

2. **Frequency**
   Every three (3) months on a calendar basis. Ad-hoc interim re-screens are triggered by negative news, UBO/ownership changes, geography or product/end-use changes, etc.

3. **Sources & Search Methodology**
   At a minimum, searches are performed in the U.S. Treasury – OFAC Sanctions List Search tool (using legal names and likely variants, personal names, and relevant address/country indicators):

   - **OFAC Sanctions List Search:** https://sanctionssearch.ofac.treas.gov/ , https://search-uk-sanctions-list.service.gov.uk/

4. **Result Validation & Escalation**
   Positive or potential matches are verified with evidence (screenshots/exports, date-time stamps, and query parameters). No new transactions are initiated until the match is conclusively cleared. Cases are escalated to Legal and Ethics & Compliance.

5. **Recordkeeping**
   Preserve all screening artifacts (screenshots/CSV exports), timestamps, search parameters, and decision/approval logs for at least five (5) years.

6. **Reporting & Monitoring**
   After each cycle, consolidate the number of customers screened, potential/positive matches, resolution lead times, and actions taken into a periodic compliance report.

7. **Contractual Flow-Down & Commercial Touchpoints**
   Where required, update contract clauses and the ABC/sanctions-compliance references in proposals and invoices; update the customer's risk score in the Compliance Risk Matrix.

3) Export Compliance Obligations

All Dell EMC products, software, and services are subject to U.S. export control laws. Therefore, TRIO distributors are required to consider the provisions of the Export Administration Regulations (EAR) in every transaction and obtain the necessary authorizations.

- The direct or indirect sale of products, software, or services to countries, entities, or individuals listed on the sanctions lists published by the U.S. Department of the Treasury's OFAC (https://sanctionssearch.ofac.treas.gov/) is strictly prohibited. Severe criminal penalties are imposed in case of violation of this rule.
- The sale of products to U.S.-sanctioned countries such as Cuba, Iran, North Korea, Syria, and the Crimea region, including indirect services provided to the embassies or consulates of these countries, is prohibited unless an official license has been obtained.
- Specifically prohibited parties include individuals on the SDN List, companies on the U.S. Entity List, terrorist organizations, narcotics traffickers, weapons of mass destruction proliferators, and organized crime groups. Transactions with these parties are strictly prohibited.
- Prohibited end uses include nuclear technology, missile and UAV systems, biological and chemical weapons development, military end use, submarine nuclear propulsion systems, and oil & gas projects related to Russia.
- Participation in boycotts not recognized by the United States is prohibited. Distributors may in no way support boycott practices imposed by third countries that are rejected by the United States, may not accept such requests, and are obliged to immediately report any such violation to TRIO.

- In all cases where a license may be required due to the product, destination country, end user, or end use conditions, the distributor is obliged to obtain the necessary U.S. export licenses and notify TRIO. Any sale without a license is considered a serious violation.

4) Export Compliance Program (ECP) – Mandatory Elements

- TRIO requires all distributors to establish a written Corporate Compliance Statement. This statement must clearly demonstrate commitment to export compliance, be known by employees, and be formally approved by management.
- A Risk Assessment must be conducted within the scope of the ECP. Distributors should review their customers, products, and intended uses to identify risks related to nuclear, military, or prohibited technologies and detect red flag indicators at an early stage.
- Party and End-Use Screening are mandatory in all commercial relationships. Customers, suppliers, and intermediaries must be screened against the U.S. Consolidated Screening List; business relationships cannot be established with prohibited individuals, entities, or suspicious addresses.
- A License Requirement Analysis must be conducted for each transaction. Considering the EAR classification of the products, the risk level of the destination country, the type of end user, and the intended use, it must be carefully determined whether an export license is required.
- Training is mandatory for all employees. Regular training must be provided on export compliance, sanctions, and red flag indicators. Senior management, consultants, and contractors should also be included in the process to ensure that corporate awareness remains continuously up to date.
- Recordkeeping is mandatory for all exports, re-export, and transfer documents. Documents must be retained for at least 5 years, with both digital and physical records securely maintained and readily accessible for audits when required.

5) Know Your Customer (KYC) Principles

TRIO must verify the identity, address, trade name, and field of activity of all business partners. Company registration documents, tax identification numbers, and contact information must be obtained in full and kept up to date.

- Third parties' beneficial owners, i.e., ultimate beneficial owners, must be identified, and the ownership structure must be clearly documented. Complex or concealed ownership structures create risks of bribery and corruption.
- Politically Exposed Person (PEP) checks must be conducted, and individuals with direct or indirect connections to public officials or their relatives must be carefully examined. Business relationships involving PEP risk require senior-level approval.

- It must be examined whether the customer or third party has previously been subject to investigations related to bribery, corruption, or trade violations. If negative findings are obtained from reliable sources, the business relationship shall be rejected.
- The business purpose and commercial activities of third parties must be clearly defined, and if there is any inconsistency between the declared activities and the products or services provided, a detailed review must be conducted. A hidden purpose is considered a red flag.
- All payment methods must be transparent and documented. Offshore accounts, cash payments, or unusual transfer channels create bribery risks. Payment terms must be clearly stated in the contract.

6) Red Flags

Location: The shipment of products to countries under U.S. sanctions such as Cuba, Iran, North Korea, Syria, and the Crimea region is prohibited. Direct or indirect sales to these countries, including to their embassies and consulates, are considered a definite red flag.

Suspicious delivery conditions are considered red flags. Addresses such as PO Boxes or UPS Stores, circuitous shipping routes, transshipment points, or shipments where the final destination is unclear may indicate that products are being diverted for the purpose of sanctions violations.

Purpose: Use in nuclear technology, missile and unmanned aerial vehicle (UAV) systems, biological or chemical weapons, military projects, and oil and gas exploration activities related to Russia is strictly prohibited. If such purposes are declared, the transaction must be rejected.

If the buyer avoids explaining the end use of the product, or if the declared use appears inconsistent with the company's line of business, a red flag arises. A concealed or disguised end use is considered a serious risk indicator.

Product: For items subject to licensing under the EAR (such as advanced encryption software or defense-related hardware), no transaction may occur without obtaining the license. Additionally, if the product is technologically far more advanced than the purchasing country's level, the transaction is deemed suspicious.

Individuals: Transactions with persons or entities listed on the U.S. Department of the Treasury's OFAC SDN List, the U.S. Department of Commerce's Entity List, terrorist organizations, narcotics traffickers, weapons of mass destruction proliferators, or organized crime groups are strictly prohibited (https://sanctionssearch.ofac.treas.gov). If the customer's name includes that of a sanctioned country, if prohibited country banks are involved in the transaction, if unusual financing methods such as cash payments are offered, or if the customer attempts to conceal their identity with falsified documents, a red flag arises.

7) Responsibilities

TRIO and its business partners are obliged to complete all necessary due diligence steps before establishing any business relationship. Identification of beneficial owners, PEP checks, sanctions screening, and license requirement analyses must be carried out in full.

The TRIO Ethics & Compliance Team is responsible for reviewing red flag findings, initiating necessary escalation processes, and overseeing transactions that require licensing. It also provides regular guidance and training support.

The TRIO Legal Department is responsible for incorporating necessary compliance provisions into contracts, executing termination procedures in case of violations, and representing TRIO in potential legal proceedings. The Legal Department is the final authority on ethical breaches.

Employees and Managers are required to comply with all provisions of this policy, immediately report suspicious situations to Ethics & Compliance, and participate in trainings. In cases of deliberate violations, individual liability applies directly.

8) Education and Awareness

TRIO provides regular training for all employees, managers, consultants, and contractors involved in export compliance and due diligence processes. The training covers current sanctions, red flag examples, and licensing procedures.

Training sessions are held at least once a year, and documented participation by employees is mandatory. Personnel without training are not permitted to take part in export, sales, or customer relations processes. This ensures that all operations are secure.

Training materials are prepared based on U.S. EAR and OFAC (https://sanctionssearch.ofac.treas.gov) regulations, Transparency International CPI reports, and TRIO Ethics & Compliance guidelines. In this way, up-to-date and practical information fully aligned with global regulations is provided.

9) Record Keeping and Auditing

All export, re-export, and transfer documents, related license applications, and customer screening results must be retained for at least 5 years. Documents must be securely preserved in either digital or physical form.

TRIO periodically audits the compliance processes of distributors. During audits, the completeness, accuracy, and timeliness of records are examined. The detection of incomplete or misleading records is considered a serious violation and triggers the sanction process.

The confidentiality of records is essential. Access is limited to authorized personnel only. Personal data is processed in accordance with KVKK and relevant international privacy regulations. Any access that violates information security standards is regarded as a severe disciplinary breach.

10) Consequences of Violations

TRIO reserves the right to immediately terminate its business relationship with distributors who act in violation of this policy. Depending on the nature of the violation, TRIO may also initiate legal proceedings and report the violation to the competent authorities.

- Individuals or entities that violate U.S. export laws may face fines of up to USD 1 million per transaction and imprisonment of up to 20 years. In addition, companies involved in violations may be banned from access to the U.S. market.
- As a result of violations, companies may lose access to U.S. financial institutions, face travel bans, and be placed on restricted lists. Such consequences create severe commercial impacts on TRIO's business partners.
- Employees bear personal responsibility in cases of intentional violations. Managers and employees involved in violations may face both disciplinary measures and legal penalties. TRIO enforces individual accountability with the utmost diligence.

11) Contact

For all questions, concerns, and violation reports, the first point of contact is the TRIO Ethics & Compliance Team. Employees and business partners are obliged to promptly report suspicious situations to the team, either in writing or verbally, without hesitation.

The official communication channels are as follows:

Ankara Branch Address: M. Kemal Mah. Dumlupınar Blv. No:266 A/33 Tepe Prime Çankaya/Ankara
Istanbul Branch Address: Nidapark Küçükyalı Mahalle B6 Daire: 18 34841 Küçükyalı-Maltepe/İSTANBUL
Email: info@triobilisim.com
Phone: +903124373535
Fax: +903124373500

All notifications received through these addresses are kept confidential and are evaluated only by authorized personnel.

TRIO protects the identity of whistleblowers and ensures they are safeguarded against retaliation. Employees or business partners have the right to confidentiality when reporting suspected sanctions violations, and security guarantees are provided.