Information Security & Data Protection Policy

Protection of company, customer and personal data; access control, incident response and records retention

Document No.	TL-POL-ISM-010	**Revision**	00
Effective date	01-10-2026	**Next review**	30-09-2027
Policy owner	IT & Service Manager (ISO/IEC 20000-1)	**Approved by**	Chairman
Scope	All information, IT systems and devices of Trade Linx, and all employees, contractors and group companies that access them	**Classification**	Public – available to all stakeholders

1. Commitment

Trade Linx (established 2005, Firm Reg. No. 2829-2005, NTN 2289271-7) supplies CIJ/TIJ industrial coding and marking printers, inks, solvents, consumables and spare parts, packaging machinery and IT equipment, and provides installation, maintenance, repair and annual maintenance contract (AMC) services. It operates from one site at 16-J Johar Town, Lahore, with 17 employees (2025).

Trade Linx protects the confidentiality, integrity and availability of its own information and of the information entrusted to us by customers, suppliers and employees, including tender documents, customer production data accessed during printer service, and personal data. We comply with the **Prevention of Electronic Crimes Act 2016** and contractual confidentiality obligations, and our IT service management is certified to **ISO/IEC 20000-1:2018**.

2. Qualitative objectives

- Only authorised people can access information, on a need-to-know basis.
- Personal data is collected only for a clear purpose, with consent where required, kept accurate and deleted when no longer needed.
- Security incidents are detected, reported and handled quickly, and lessons are learned.
- All employees know their information security responsibilities.

3. Controls

3.1 Access control

- Unique user accounts, strong passwords (minimum 12 characters) and multi-factor authentication for email and cloud systems.
- Access rights are approved by the manager, reviewed every six months, and removed on the day an employee leaves.

3.2 Devices and network

- Firewall on the office network, licensed antivirus on all computers, automatic security updates, encrypted laptops, and a separate guest Wi-Fi.
- Daily backup of accounting and sales data, with a monthly off-site/cloud copy and a restore test every quarter.

3.3 Third-party and customer data

- Customer data (contact details, contracts, drawings, product/batch data from coding printers) is used only to deliver our service, is never sold, and is shared with third parties (e.g. a manufacturer for warranty) only when needed and under a confidentiality agreement.
- Service engineers do not copy customer files or production data from a printer or PC unless the customer asks in writing.

3.4 Consent

Personal data of employees, job applicants and customer contacts is collected with a written consent/notice stating what is collected, why, who it is shared with and how long it is kept (consent form in Annex A). Individuals may ask to see, correct or delete their data by writing to **akhtar@tradelinx.pk**; requests are answered within 30 days.

3.5 Records retention schedule

Record	Retention period	Disposal method
Accounting, tax and sales invoices	10 years	Shredding / secure delete
Tender and contract files	Contract end + 6 years	Shredding / secure delete
Personnel files, payroll	Employment end + 6 years	Shredding / secure delete
Job applications (not hired)	1 year	Shredding / secure delete
Service reports and customer records	Contract end + 6 years	Secure delete
CCTV recordings	30 days	Automatic overwrite
Security incident records	3 years	Secure delete

3.6 Incident response plan

#	Step	Action (responsible: IT & Service Manager)
1	Report	Anyone who suspects an incident (lost laptop, phishing click, virus, data sent to wrong person) reports it immediately to IT (Muhammad Saqib) at saqib@tradelinx.pk.
2	Contain (within 4 h)	Disconnect affected device, reset passwords, block accounts.
3	Assess (within 24 h)	Decide what data is affected and how serious it is; inform the Chairman.
4	Notify	Inform affected customers/individuals and, where required, authorities (e.g. FIA Cybercrime Wing) without undue delay.
5	Recover	Restore from backup, check systems are clean.
6	Learn	Record the incident, root cause and corrective action in the incident register; review at management review.

4. Quantitative targets

KPI	Baseline (2025)	Target	Target year
Employees trained on information security and data protection	100%	100% every year	2026
Information security risk assessment updated	None – introduced 2026	Every year	2026

KPI	Baseline (2025)	Target	Target year
Security incidents contained within 24 hours	n/a (no incidents in 2025)	100%	2026
Confirmed data breaches involving customer or personal data	0	0 every year	Annual
Phishing-simulation click rate	Not tested (first test 2027)	< 10%	2027

5. Governance, reporting and review

The **IT & Service Manager Muhammad Saqib** (Accounts Manager, also responsible for IT) owns this policy, keeps the information security risk assessment and incident register, and reports quarterly to the Chairman. Concerns can also be raised confidentially and without retaliation through the Whistleblowing & Grievance Procedure TL-SOP-GRV-010. Breaches of this policy lead to disciplinary action. The policy is reviewed at least once a year.

Approval

This document was approved by the Chairman of Trade Linx on 01-10-2026 and is effective from that date. It is communicated to all employees and relevant stakeholders, applies until superseded and is reviewed at least annually.

Prepared by: IT & Service Manager (ISO/IEC 20000-1)

Approved by	Signature and company stamp	Date
Chairman, Trade Linx	Approved and signed by the Chairman – signed original held at Trade Linx Head Office, Lahore	01-10-2026

Revision history

Rev.	Date	Description of change	Approved by
00	01-10-2026	First issue.	Chairman

Annex A – Data processing notice and consent form

Trade Linx collects your name, CNIC, contact details, bank details, education and employment history for employment, recruitment or customer service. It is shared only with banks, PESSI/EOBI, tax authorities and insurers as needed and kept for the period in the retention schedule. You may ask to see, correct or delete your data at akhtar@tradelinx.pk.

I consent to the processing of my personal data as described above.

Name: _____ CNIC: _____ Signature: _____ Date: _____