

Risk Management and Information Security Policy

Soysal International İç ve Dış Ticaret Limited Şirketi

Version	1.0 (October 2026)
Approved by	Emrullah Soysal, CEO
Effective date	5 October 2026
Policy owner	CEO
Review	Annually; the risk register is reviewed quarterly

Part A — Risk management

A1. Approach

We identify, assess and manage the risks that could stop us from delivering to customers safely, legally and profitably. Our process follows the principles of **ISO 31000** and is scaled to the size of our company.

A2. Process

1. Identify: keep a risk register covering:

- commercial risks (customer credit, currency, supplier failure);
- compliance risks (sanctions, export controls, bribery, fraudulent documents);
- social and ethical risks (forced labour or child labour in the supply chain);
- environmental risks (dangerous goods, spills, carbon);
- health and safety risks;
- information security risks;
- logistics and country risks.

2. Assess: rate each risk by likelihood (1–5) × impact (1–5). A score of 12 or more is "high".

3. Treat: for every high risk, record an owner, controls and actions with deadlines.

4. Before any new activity we add a risk assessment to the register: a new product category, a new country, a new customer type, a tender, or a new supplier rated medium or high risk.

5. Monitor: the CEO reviews the register **quarterly** and after any incident.

6. Report: the top risks and actions are summarised in the annual management review.

A3. Key standing controls

Risk	Control
Sanctions and export controls	Customer and end-user screening before quotation and before shipment
Payment and credit	Advance payment or a confirmed letter of credit for new customers; credit insurance when available

Risk	Control
Supplier non-delivery or quality	Onboarding checks (Policy 06); pre-shipment inspection for high-value orders
Fraudulent documents	Verify certificates with the issuer for high-value or critical orders
Bribery	Policy 02 controls
Forced or child labour	Policies 03 and 06
Currency	Quote in the customer's contract currency; review exposure for long delivery times

Part B — Information security and data protection

B1. Scope

Part B covers information about the Company, its customers, suppliers and employees held in any form, including:

- email and cloud accounts (Google Workspace);
- laptops and phones;
- the website and online forms;
- the supplier portals we use.

B2. Operations — controls in our own company

1. Access:

- individual accounts only, no shared passwords;
- **multi-factor authentication** on email, cloud storage, banking and supplier portals;
- access removed on the last working day.

2. Passwords: a password manager; unique passwords of at least 12 characters.

3. Devices:

- automatic OS and software updates;
- full-disk encryption;
- screen lock;
- antivirus or built-in protection enabled;
- lost devices reported immediately and wiped remotely where possible.

4. Email security:

- SPF, DKIM and DMARC set up on soysalinternational.com;
- staff are trained to spot phishing and **invoice-change fraud**;
- **any change to bank details is confirmed by phone** using a number already on file.

5. Backups: business data is held in the cloud with version history; critical files are also backed up separately.

6. Website: hosted on a managed platform with HTTPS and security headers. Forms are protected against spam and bots. No payment card data is stored.

7. Incident response:

1. Contain the incident by changing passwords and isolating the device.

2. Assess what data is affected.
3. Notify affected customers or suppliers.
4. Notify the Personal Data Protection Authority (KVKK) **within 72 hours** where personal data is breached.
5. Record the incident and the lessons learned.

B3. Products — what we supply

For IT hardware, networking and electronic products:

- we source only from authorised manufacturers or distributors;
- we supply products in their original sealed packaging, with firmware from the manufacturer;
- we keep serial-number records to fight counterfeit and tampered products.

B4. Suppliers and subcontractors

- Suppliers that handle our or our customers' data must protect it. Our Supplier Code of Conduct requires them to protect confidential information and personal data against cyber threats.
- We share only the information a supplier needs for the order. Customer identities and end-destinations are shared only when necessary.
- IT service providers (cloud, website, accounting software) are chosen from reputable providers with recognised security certifications (for example ISO 27001 or SOC 2) and data-processing terms that comply with KVKK.

B5. Personal data (KVKK)

We process personal data lawfully and transparently under Law No. 6698. The privacy notices published on soysalinternational.com explain:

- the data controller;
- the purposes and legal bases of processing;
- how long data is kept;
- the rights of data subjects.

B6. Training

All employees complete information security and phishing-awareness training when they join and every year, as part of the annual ethics and compliance training.

Approved by Emrullah Soysal, Chief Executive Officer, on 5 October 2026. A signed copy is held by the Company.