isotrading
quality & timing sourcing

17 rue du Colisée, 75008 Paris FRANCE
☎ + 33 (0) 1 7894 5610
www.isotrading.com

Data Protection Policy

Data protection and security provisions are extremely important to meet our customers, suppliers, and internal users' confidentiality regulatory requirements, and thus mitigate the risks to personal data.

The 7 data processing and protection principles:

- Legality, fairness and transparency
- Limitation of purposes
- Data minimization
- Accuracy and timely updating
- Limitation of storage
- Integrity and confidentiality
- Accountability.

As a result, we have decided to restrict access to confidential and sensitive data to prevent it from being compromised or lost, so as not to harm our partners and staff, while allowing users to access the data they need to work effectively.

This policy applies to all customer data, personal data or other data defined as sensitive by Isotrading.

It therefore applies to all servers, databases and computer systems that process this data and to any user who interacts with the company's computer systems.

Information classified as public is not subject to this policy.

Each user will only be granted the access rights they need to perform their job.

User access records may be used as evidence in the investigation of a security incident.

Users must lock their screens each time they leave their workstation, not leave any sensitive or confidential information visible and not share their passwords.

The IT department must inform Management immediately of any IT security incident.

Complaints must be recorded in the QMS.
Any user who violates this policy is subject to disciplinary sanctions.
This policy must be reviewed at least once a year.