connect with confidence.

CiS Group Ethics and Compliance Policy
(Anti-corruption, money laundering, fraud, conflicts of interest, data protection, and supplier ethics)

1. Purpose of the Policy

This Ethics and Compliance Policy specifies the principles set out in the Code of Conduct and describes our company's expectations regarding ethical, responsible, and legally compliant conduct. Our company is committed to maintaining high ethical standards in all business activities. Corruption, fraud, money laundering, and inappropriate conflicts of interest will not be tolerated.
The purpose of this Policy is to:

- avoid legal and reputational risks
- promote a culture of integrity and transparency
- support employees in making ethical decisions
- ensure responsible and sustainable business practices

This Policy forms part of our compliance management system and is supported by supplementary processes, procedures, and internal regulations.

2. Scope of Application

This Policy applies to all employees.
In addition, we expect business partners, suppliers, consultants, and other persons acting on behalf of our company to comply with comparable ethical standards.
All managers of the CiS Group bear a particular responsibility for leading by example in accordance with this Policy and promoting a corporate culture in which integrity and responsible conduct are a matter of course.

3. Principles of Ethical Conduct

All employees are required to:

- comply with applicable laws and regulations
- make business decisions objectively and in the interests of the company
- ensure transparency and fairness in business dealings
- protect company´s values and assets
- identify and report potential violations of these principles at an early stage

Integrity and responsible conduct form the basis for sustainable economic success and trusting business relationships.

4. Anti-Corruption

The CiS Group has a zero-tolerance Policy towards corruption and bribery.
It is prohibited to offer, promise, grant, or accept benefits, either directly or indirectly, in order to influence business decisions or obtain an unfair advantage. This applies in particular to:

- monetary payments or benefits in kind
- inappropriate gifts or invitations
- indirect benefits provided through intermediaries or third parties

Gifts and Invitations

Gifts or invitations may only be accepted or provided if they:

- are customary in the ordinary course of business
- do not influence business decisions
- are transparent and appropriate

As a guideline, an appropriate value is a maximum of EUR 30 to 50.

5. Fraud Prevention

Fraud, deception, or the misuse of company resources are strictly prohibited. This includes, in particular:

- manipulation of invoices or financial records
- false expense claims
- procurement or supplier fraud
- theft or misuse of company assets
- intentional misrepresentations in reports or documentation

All employees are required to report irregularities or suspicious activities.

6. Prevention of Money Laundering and Terrorist Financing

Our company does not participate in money laundering or terrorist financing, either directly or indirectly. Employees must be particularly vigilant with regard to:

- unusual or complex payment structures
- transactions without a clearly identifiable economic purpose
- unusually high cash payments
- business relationships involving opaque corporate structures
- countries or persons listed on sanctions, embargo, or counter-terrorism lists

Suspicious activities are reviewed and reported in accordance with internal processes.

7. Conflicts of Interest

Conflicts of interest arise when personal interests conflict or could conflict with the interests of the company. Employees must avoid situations in which personal benefits could influence their professional decisions. Examples of potential conflicts of interest include:

- business relationships with companies in which employees or their family members have an interest
- secondary activities that could influence business decisions
- personal benefits arising from business relationships

Potential or actual conflicts of interest must be disclosed at an early stage.

8. Data Protection and Information Security

The protection of personal data and confidential company information is of great importance to our company. Employees are required to:

- process personal data only within the scope of the applicable data protection laws
- protect confidential company information
- make sensitive information accessible only to authorised persons
- use IT systems and data responsibly

Unauthorised access, misuse of data, or the disclosure of confidential information is prohibited. These requirements must also be observed, in particular, when working remotely and while on business trips.

9. Responsibility Towards Suppliers and Business Partners

The CiS Group does not maintain business relationships with sanctioned persons or companies, or in regions subject to international embargoes or prohibitions. When selecting business partners, suppliers, and customers, we ensure that no business is conducted in such regions in violation of applicable sanctions or statutory requirements. Expectations towards business partners:

- compliance with laws and regulations
- prevention of corruption and bribery
- fair business practices
- responsible handling of data and information

Integrity and responsible conduct are key criteria in the selection of and cooperation with business partners.

10. Reporting Violations

All employees are encouraged to report possible violations of laws, internal policies, or ethical standards. Reports can be submitted through the following channels:

- direct supervisors
- management
- the external whistleblowing system operated by an independent ombudswoman

The ombudswoman acts as an independent reporting office and ensures that reports are handled confidentially and in accordance with legal requirements. Persons who submit reports in good faith are protected against discrimination or retaliation.

11. Implementation and Processes

The implementation of this Policy is supported by internal processes and procedures, in particular:

- processes for reporting and investigating compliance violations
- procedures for disclosing conflicts of interest
- processes for screening business partners
- internal training and awareness-raising measures

12. Training and Awareness

Our company promotes compliance with this Policy through regular information and training for all employees.

13. Consequences of Violations

Violations of this Policy may have consequences under employment law and other legal consequences. Depending on the severity of the violation, measures may include:

- disciplinary measures
- employment-related consequences, up to and including termination of employment
- claims for damages
- criminal proceedings

Reports of possible violations are carefully investigated.

14. Responsibility and Review

The management is responsible for implementing this Policy.

The Policy is reviewed regularly and updated as necessary to comply with legal requirements and international standards of responsible corporate governance.