



UAB "SCT LUBRICANTS" CONFIDENTIALITY POLICY

Updated September 2024



CONFIDENTIALITY POLICY

A Confidentiality Policy helps to protect confidential information, including trade secrets, business strategies, and proprietary data. It sets clear expectations for employees, mitigates risk of information leaks, and potentially prevents legal disputes and financial losses.

What is a Confidentiality Policy?

A Confidentiality Policy is a set of guidelines that outline how employees at UAB “SCT Lubricants” should handle sensitive and proprietary information. It's crucial to protect company's intellectual property, trade secrets, and other confidential data. Confidentiality Policy helps ensure that employees understand their responsibilities and the potential consequences of disclosing sensitive information.

What Confidential Information Is

The confidential information will include all data and information relating to the business and management of the Employer, including but not limited to, client data, business strategies, marketing plans, proprietary and trade secret technology and accounting records to which access is obtained by the Employee, including work product, computer software, other proprietary data, business operations, marketing and development operations, and customer information.

The confidential information will also include any information that has been disclosed by a third party to the Employer and is governed by a non-disclosure agreement entered into between that third party and the Employer.

What Confidential Information Is NOT

The Confidential Information will not include information that:

- Is generally known in the industry of the Employer;
- Is now or subsequently becomes generally available to the public through no wrongful act of the Employee;
- The Employee rightfully obtains from a third party who has the right to transfer or disclose it.



LIST OF CONFIDENTIAL INFORMATION

Personal data

All data as defined in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter referred to as the "General Data Protection Regulation") and the Law on Legal Protection of Personal Data of the Republic of Lithuania, which correspond to the definition of personal data and personal data of special categories, and which are processed by the Company.

Employee's personal data

The remuneration specified in the Company's employees' employment contracts, the personal files and the information collected and stored therein, the results of compulsory medical examinations, the personal information specified by the employee (health data, residential address, personal telephone number, marital status, age, etc.), with the exception of the average salary of groups of employees distinguished by qualification levels.

Information relating to staff changes

Planned changes in staff management, planned reductions or increases in posts, redundancies of specific staff, etc. The number of employees of the Company and information on changes in personnel management implemented shall not be considered as confidential information.

Customer information

Information relating to natural and legal customers. The Company's lists of Customers, suppliers, partners, terms of sale and purchase, contracts, sales prices, Customer discounts, cost of products and services, sales methods, management reports, management principles, knowledge of pricing structure, costs, internal price lists and tariffs, plans to participate in tenders, auctions, bids for tenders and related material.

Electronic banking data

For the use of electronic banking, the Company's responsible employees are provided with individual passwords and codes, the system for their provision, and the Company's other electronic banking data (bank account balances etc.).



Accounting data Any information concerning the accounting data and financial records of the Company and its customers, in particular documents relating to assets, banking transactions, international settlements, receipts and income, receipts on account or cash, interest paid, the financial position of the Company and its customers, budgets, except for aggregated information provided to public authorities in the form of financial statements.

IT systems and databases The information systems and applications used by the Company, the structure of the computer networks, the hardware and software of the computer networks, the structure of the files, the backups of the data and the information contained therein, as well as the passwords and user logins or other security codes used and other security measures. The Company's databases contain customer and employee information, the loss of which could jeopardize the Company's operations or cause loss to the Company.

Information on negotiations, the Company's business plans, external and internal audits, legal proceedings. Information on negotiation tactics, powers of persons delegated to negotiations, information on signed letters of intent, plans to participate in tenders, auctions, bids for tenders and related material. Information and results of the Company's external and internal audits as well as other inspections, as well as information on the Company's participation in legal proceedings, unless the court decides to hold a public hearing.

Decisions of the Company's shareholders The content of the decisions taken by the Company's shareholders.

Information that is identified as confidential in transactions or by the supplier The terms of transactions entered into by the Company and information concerning the performance of those transactions, if the terms of the transactions make that information confidential, and information received by the Company that has been designated as confidential by its supplier.

Technological solutions and professional and trade secrets New ideas, know-how, new technical solutions, inventions in the pipeline, scientific, technical, structural and technological solutions, trademarks and other information of commercial value of the Company.



Information on the safety and security of the Company's assets and infrastructure objects	Security system (security service data, alarm codes, passwords used in communication with the security service); technical documentation and instructions for the security and alarm system of the Company's premises and the protected area, cars, other assets; as well as other information, the disclosure of which may lead to unauthorized use of technical equipment or access by third parties to the Company's facilities or protected area.
Internal legislation and other internal documents	All internal legislation and internal documents of the Company shall be treated as confidential, except where such documents have been prepared with a view to public disclosure or, in the opinion of the drafter, are capable of being disclosed.
Production and other information	The results of laboratory tests carried out by the Company, information on the production process, technology, equipment, personnel.
Regarding the provision of confidential information to the external audit	The external audit shall be provided with all the necessary information provided for in the Law on Audit of Financial Statements of the Republic of Lithuania, Regulation (EU) No 537/2014 of the European Parliament and of the Council.

Confidentiality Policy part of the employee's handbook

The Confidentiality Policy is a part of UAB "SCT Lubricants" employee's handbook. This policy is a living document and is updated as necessary to reflect changes in laws, regulations, and business practices.

Scope

We expect all employees at UAB "SCT Lubricants" to follow this policy.



POLICY ELEMENTS

Handling Confidential Information

We expect our employees to handle confidential information responsibly and to ensure that such information is not disclosed to unauthorized individuals or entities. Confidential information includes, but is not limited to, trade secrets, business plans, customer lists, financial data, and proprietary technology.

We advise our employees to:

- Understand what information is considered confidential.
- Not disclose confidential information without proper authorization.
- Securely store and dispose of confidential information.
- Report any suspected breaches of this policy immediately.

Representing our Company

Some employees may be required to discuss confidential information with clients, vendors, or other third parties. In these cases, employees should:

- Only disclose the necessary information
- Ensure that the third party understands the confidential nature of the information
- Seek to have the third party sign a Non-Disclosure Agreement when appropriate

Data Security

- All employees must ensure that confidential information is stored securely, whether in physical or electronic form.
- Physical documents should be kept in locked cabinets, and electronic files should be password-protected and encrypted when necessary.
- Unauthorized duplication, reproduction, or removal of confidential information is strictly prohibited.

Reporting and Breach Notification

- Employees must promptly report any suspected or actual breaches of confidentiality to their supervisor or the designated person responsible for handling such cases.
- The company will investigate all reported breaches and take appropriate actions to address the situation, including disciplinary measures and legal actions if necessary.

Disciplinary Consequences

We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee Confidentiality Policy include but are not limited to:

- Unauthorized disclosure of confidential information.
- Failure to properly secure confidential information.
- Failure to report known breaches of this policy.



UAB „SCT LUBRICANTS“
Silutes st.119, 95112
Klaipeda, Lithuania
tel.: +370 46 340 345
e-mail: klaipeda@sct.lt

www.sct-lubricants.com