Information Security Policy of Pröll GmbH

1. Company and Business Purpose

Pröll GmbH develops, produces, and distributes customer-specific functional printing inks and lacquers for screen and pad printing technology worldwide.
Research and development take place in the central laboratory, and production occurs in two separate production halls, exclusively at the location in Weissenburg i. Bay.
Sales are handled by the subsidiary companies Pröll Services GmbH in Germany and Austria, Proell, Inc. St. Charles IL in the USA, Canada, and Central America, Proell Ink Trading Shanghai Co. Ltd. in China, as well as independent dealers in other countries.
Since the company daily works with sensitive data and products, it is of great importance to implement a comprehensive IT security concept. This IT security policy serves as a guideline for all employees and aims to ensure that the company's IT systems and data are optimally protected.
For better readability, this policy avoids the simultaneous use of male, female, and diverse (m/f/d) language forms. All terms apply equally to all genders.

2. Scope

In the interest of our customers and a functioning supply chain, alongside the production and delivery of high-quality printing inks and lacquers, the proof of quality and security of internal processes is also required.
For this reason, we have developed an information security policy that aims to fulfill this requirement. The policy includes guidelines to ensure the secure processing of information within our company. It applies to all areas and departments and serves as a directive for the entire company. By implementing this policy, we ensure secure information processing and aim to achieve the necessary quality and security level required for successful competition.

3. Requirements, risks and goals

The goals of IT security are compliance with the relevant legal regulations, particularly data protection, the protection of business secrets, especially formulation and production know-how, and trade secrets based on long-standing confidentiality agreements with customers and suppliers, as well as the prevention of operational interruptions or damage due to electronic attacks from outside (cybersecurity).
In this context, the business success of our company depends on identifying existing risks to the aforementioned goals, mitigating or avoiding them through appropriate measures, and
an adequately handling of any remaining risks.

4. Importance of Security

Given external and internal requirements, especially the security requirements of our customers, information security must be an integral part of our company culture.
For Pröll GmbH, information security represents a very important quality characteristic of data processing since all essential strategic and operational business processes within the company are significantly supported by information technology (IT).
Disruptions to the availability of the company's applications can have serious consequences, as can irregularities regarding the integrity and confidentiality of the information processed or used. The availability, confidentiality and integrity of information, applications and IT systems are threatened not only by external factors but can also be endangered by internal vulnerabilities.
Every employee must be aware of the necessity of information security and understand the fundamental impact of risks on business success.

5. Responsibilities

In accordance with this policy, each organizational unit of Pröll GmbH is initially responsible for the security of its own data and its processing ("information owner"). As part of this responsibility, the IT department, together with each organizational unit, will compile a list of their assets (data, systems, and processes), conduct a risk analysis and assessment according to a prescribed uniform template, and update it regularly and after significant changes.

5.1 Management

As the highest decision-making body, the management is responsible for adopting this information security policy.
It ensures that the information security management system (ISMS) is implemented and regularly updated according to this policy. For this purpose, the IT department is provided with sufficient financial and time resources to continue education, stay informed, and achieve the management’s security goals.
Management is also responsible for reviewing and approving the ISMS at least once a year (or in the case of significant changes).
This review serves as proof of the adequacy, suitability and effectiveness of the ISMS. Overall responsibility for the proper and secure fulfillment of tasks, including information security, lies with company management.

5.2 IT-Department

The IT administrator, who reports directly to management, is responsible for the implementation. The administrator, together with the department heads of Pröll GmbH named in the “Business Area Organizational Chart,” as well as the branch managers
or managing directors of the sales subsidiaries, must carry out all necessary IT security measures.

These include, in particular, updating hardware and software, ensuring data traffic safety, raising user awareness to maintain confidentiality during data exchange and data protection, identifying dangers in internet usage, warning of attacks on IT infrastructure, and regular training of all users on security-related matters.
The IT department is tasked with controlling and restricting access to sensitive systems, security zones, and critical infrastructure using appropriate technical, organizational, and infrastructural measures. This includes access to important information and applications, which should only be granted to authorized persons. Information owners are also involved in this process.
The IT department is also responsible for ensuring the confidentiality, integrity, availability, and authenticity (where applicable) of data and systems. This is achieved through the creation and implementation of a security concept, which, based on risk assessments, provides for appropriate measures to prevent unauthorized access, manipulation, or failures.

5.3 Data Protection Officer

The organization has appointed a Data Protection Officer (DPO). The DPO is involved in the development of the information network and handles all questions related to data protection within a dedicated Data Protection Management System (DPMS).

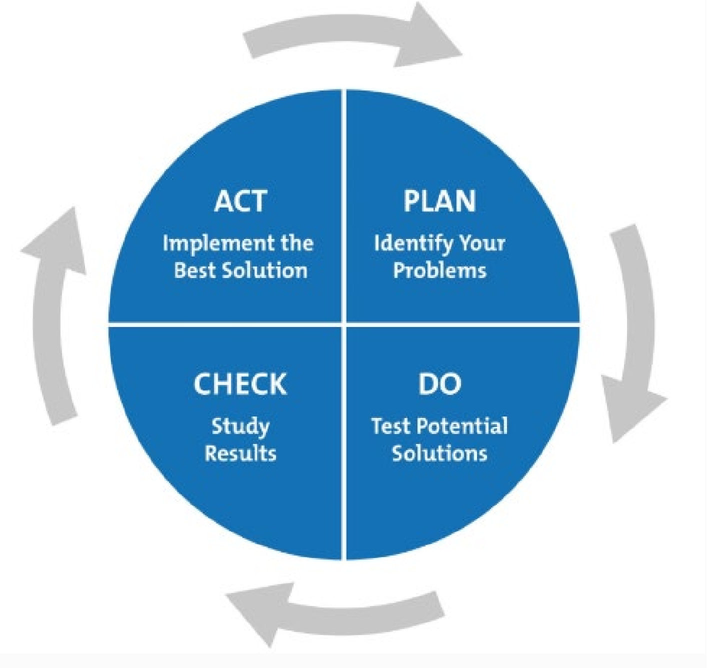
5.4 Employees

The employees of our company must always be aware of the importance of information security and actively participate in preventing and combating material and immaterial damages. They should handle the information systems and the data stored and processed on them responsibly and pay attention to the confidentiality of trade and business secrets.
Employees will be provided with specific security rules for their respective workplaces when needed and must regularly participate in the security training offered.
In the event of irregularities, employees are required to immediately inform the IT department and their respective supervisors. It is expected that every user of IT systems
is familiar with and adheres to this information security policy.

6. Commitments

Management will actively support the security organization and the security process.
Our company will align itself with the ISO 27001 standard and the IT-Grundschutz methodology and implement the management elements of these standards. These include conducting regular internal audits, appropriate management of documentation and records, management reviews, and applying the continuous improvement model (PDCA).
Each employee is required to observe and comply with the general and workplace-specific security guidelines.

This security policy generally applies internally. If necessary, management will decide whether third parties (e. g., customers, contractors, suppliers) should be involved.
This policy becomes effective upon the signature of management and internal publication.



Weißenburg i. Bay., 21. August 2024

____

Reinhard Port
(General Manager)