	INFORMATION SECURITY POLICY PILOUS spol. s r.o.	ISMS Policy
		PILOUS spol. s r.o. IČO: 47535709

The company PILOUS spol. s r.o. announces the Information Security Policy as a set of main principles and measures with the aim of ensuring the protection of the company's important information assets, which are a key resource for the fulfillment of the company's strategy.

Information Security Subject

By information assets, we mean the information needed to ensure the essential activities of the company and all the resources that are necessary for the creation, processing, storage and use of information as well as for its own protection. These are mainly data, information, software, hardware, end-devices (computers, laptops, printers, barcode readers, etc.), infrastructure (networks, network devices, etc.), people (internal and external workers who hold unique knowledge or those handling key information assets), suppliers (HW, SW administrators, etc.). Information assets also include information processed in other than electronic form (printed documents and records, record books, video recordings from security cameras, etc.). To ensure information security, we identify important information assets and all aspects that may threaten these assets. We take reasonable measures to ensure the required availability, confidentiality, integrity and authenticity of these assets.

Target Groups


The company's information security management affects all stakeholders, especially all internal and external employees, suppliers and customers. Anyone who comes into contact with the company's information assets must be aware about this policy and, to the necessary extent, must be aware about the specific requirements, rules and procedures for handling information assets contained in the company's management documentation.

Information Security Principles

All essential aspects of information security are documented in the company's internal management documentation. They are regularly reviewed, updated and approved by the company's management and form a unified information security management system. The CEO of the company is responsible for information security at the highest level. The Information Security Manager is responsible for the methodical leadership and management of information security.

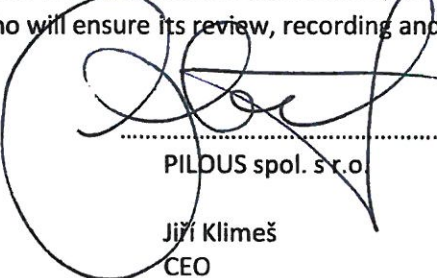
Main Principles of Information Security are:

1. The company adopts and enforces the measures necessary to ensure information security based on best practice and in accordance with the recognized ISO 27k series information security standards.
2. The company's information assets are identified as part of a risk analysis and assessed in terms of possible impacts on the company in the event of a breach of their availability, integrity and confidentiality.

 PILOUS PACKAGING	INFORMATION SECURITY POLICY PILOUS spol. s r.o.	ISMS Policy
		PILOUS spol. s r.o. IČO: 47535709

3. Information is always classified and indicated by its degree of confidentiality.
4. The use of information assets is always managed in accordance with their classification, including access control. Access to information assets is always granted solely on the basis of the purpose for which they are used. If the purpose of use of the information asset ceases, access must be revoked.
5. Protection of the physical environment provides a sufficient basis for the protection of information assets.
6. End users of information assets are instructed on the prescribed procedures and rules in connection with their use.
7. Suppliers and customers are aware about the information security management system to the extent necessary to ensure the security of information assets used in supplier-customer relations with the company, including ensuring the security of information of the company's customers used for the fulfillment of deliveries. Substantial aspects of information security within supplier-customer relationships are contractually regulated.
8. Any breach of information security or even suspicion of such a breach must be immediately reported by all interested parties to the information security manager, who will ensure its review, recording and resolution.

In Praha on 4. 4. 2023



 PILOUS spol. s r.o.
 Jiří Klimeš
 CEO