INFORMATION
SECURITY POLICY

AIMS OF THE SECURITY POLICY

Our primary goal is to ensure the complete confidentiality, integrity and availability of our own and customer data to ensure the smooth running of our business activities. With this policy, we declare to all business partners, employees, the public and state administration and the general public the ability of Skrivanek Holding SE to effectively protect information, tangible and intangible assets owned and entrusted to us in accordance with legislative requirements in every country where we operate.

INFORMATION SECURITY PRINCIPLES 1/3

We commit to:

comply with and uphold the legislation in the field of information security in all countries where our group operates, ensure the availability of timely and location-specific information according to societal needs, but to only supply this information to those needing it for their work, thus maintaining the confidentiality of information according to specified categories – public, internal, confidential, personal.

SKRIVANEK

MANAGEMENT STATEMENT

Skrivanek is the leading provider of language services in the field of translations and interpreting, localization, DTP services and language tuition in the Czech Republic and 13 other countries throughout the world.

The management of Skrivanek Holding SE announces this Information Security Policy as a framework for the Company's direction in the field of information security protection. The management's intention is to support the set goals and principles of this policy.

INFORMATION SECURITY PRINCIPLES 2/3

We also commit to:

manage the integrity and life cycle of information from the moment of its creation, transfer, and use to its disposal,

to educate and develop our employees, suppliers and partners in the field of information security, whereby the violation of information security rules is considered a gross violation of internal regulations and contractual relationships.

SECURITY POLICY CERTIFICATION

To enforce the policy, the Company has introduced and developed an information security management system according to ISO/IEC 27001:2022. This is an international standard for information security management systems. It provides protection against potential security threats such as cybercrime, misuse of personal data, vandalism/terrorism, fire/damage, misuse and data theft / virus attack.

INFORMATION SECURITY PRINCIPLES 3/3

We further commit to:

determine security measures based on the principle of assessing the severity of risks, their impacts and economic effects, regular monitoring, risk reassessment,

management of security events and incidents through corrective and preventive measures to increase the effectiveness of our information security management system.

2020 - **2024**

Suggested: OLO Approved: BCH 2. 1. 2024