INFORMATION SECURITY POLICY (2025 – 2027)

SKRIVANEK

MANAGEMENT STATEMENT

Skrivanek, as a leading provider of language-tech services, declares this Information Security Policy as the foundation for safeguarding business operations and stakeholder trust.

Through the implementation and continuous development of our Information Security Management System (ISMS), aligned with ISO/IEC 27001:2022, we aim to:

- Protect against emerging threats, including cybercrime, AI-driven risks, and data misuse.
- Ensure compliance with applicable international and local regulations, maintaining a proactive approach to changes in legislation.
- Cultivate a security-first culture across all levels of the organization.
- The management supports this policy by providing resources, leadership, and strategic oversight to ensure its implementation, regular review, and alignment with global best practices.

AIMS OF THE SECURITY POLICY

1. Strengthen measures to address emerging cybersecurity threats, including ransomware, phishing, and AI-driven attacks.
2. Enhance compliance with global and regional data protection regulations (e.g., GDPR, CCPA, and new local requirements).
3. Continuously improve risk assessment and incident response processes to align with best practices in information security.
4. Promote a culture of security awareness among employees, suppliers, and partners.

PRINCIPLES

We Commit To:

- Complying with and upholding information security legislation across all countries where our group operates.
- Ensuring information availability at the time and place required for business operations while restricting access based on the principle of least privilege.
- Classifying and handling information as public, internal, confidential, or personal, with strict access controls at every level.
- Strengthening access management protocols through multi-factor authentication (MFA) and role-based access controls (RBAC) to minimize unauthorized access risks.
- Managing the integrity and lifecycle of information — from creation and transfer to secure disposal — ensuring all processes align with international standards.
- Continuing with regular trainings and implementing mandatory annual programs tailored to job roles, focusing on emerging threats and secure data handling to ensure organization-wide awareness and preparedness.
- Treating violations of information security rules as gross breaches of internal regulations and contractual agreements.
- Implementing mandatory annual training programs tailored to job roles, focusing on emerging threats and secure data handling to ensure organization-wide awareness and preparedness.
- Determining security measures based on risk severity, their impacts, and cost-effectiveness, ensuring proportional and adaptive security.
- Regularly monitoring risks, reassessing threats, and applying corrective and preventive measures to continuously improve the ISMS.
- Expanding incident response capabilities, including real-time detection, reporting, and remediation strategies to minimize downtime and impact.
- Integrating AI-driven threat detection and response systems for faster identification and mitigation of breaches, enhancing the overall resilience of our information security framework.