



Information Security Policy

KPMG in Slovakia

Aligned with ISO/IEC 27001:2013



1 Objectives

The management team of KPMG in Slovakia are committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout KPMG in Slovakia in order to preserve and safeguard the firm's corporate and client data, systems, applications, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements continue to be aligned with KPMG in Slovakia's goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for reducing information-related risks to acceptable levels.



2 Policy Statement

KPMG in Slovakia's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The National IT Security Officer is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Computer system resources and associated corporate data are business critical KPMG assets requiring a high level of protection. It is KPMG in Slovakia's policy that sufficient measures should be taken to protect these assets against accidental or unauthorized modification, disclosure or destruction, as well as to assure the confidentiality, integrity and availability of KPMG's automated data processing activities.

The Management of KPMG in Slovakia, represented by its Managing Partner, declares its Information Security Policy following the requirements of ISO/IEC 27001:2013, which is accessible, understood, implemented and maintained by the personnel at all levels in the Organization.

The Management recognizes its responsibility in development, implementation, maintenance and continual improvement of Information Security Management System (ISMS), compliant to the requirements of ISO/IEC 27001:2013 and applicable legal and regulatory requirements.

The Management of KPMG in Slovakia confirms that KPMG in Slovakia has the necessary resources for the development and continual improvement of the ISMS and will be responsible for raising the personnel and management awareness of the implementation of the Information Security Policy and its objectives.



3 Scope

All employees of KPMG in Slovakia are expected to comply with this policy and with the ISMS that implements this policy. The policy is mandatory at KPMG in Slovakia.

The ISMS is subject to continuous, systematic review and improvement.

KPMG in Slovakia has established an IT Security organization, chaired by the CIO and including the National IT Security Officer and specialists in different security areas to support the ISMS framework.

This policy is reviewed at least annually, or when and if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

The National IT Security Officer is the Owner of the Information Security Policy and has approved management responsibility for the development, review and evaluation of the policy.

A current version of this document is available to all KPMG in Slovakia employees on the corporate intranet. It does not contain confidential information and can be provided to relevant external parties upon request.

Contact us

Kenneth Ryan

Managing Partner

T +421905752752

E kenneth.ryan@kpmg.sk

Robert Jarolin

National IT Security Officer

T +421905720227

E rjarolin@kpmg.sk

www.kpmg.sk

© 2020 KPMG Slovensko spol. s r.o., a Slovak limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.