ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Júl 2022

STN	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Sektorovo špecifická aplikácia pre ISO/IEC 27001 Požiadavky	STN ISO/IEC 27009 97 4152

Information security, cybersecurity and privacy protection
Sector-specific application of ISO/IEC 27001
Requirements

Sécurité de l'information, cybersécurité et protection des données personnelles
Application de l'ISO/IEC 27001 à un secteur spécifique
Exigences

Informationstechnik – IT-Sicherheitsverfahren
Sektorspezifische Anwendung der ISO/IEC 27001
Anforderungen

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 27009: 2020 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International Standard ISO/IEC 27009: 2020 and has the status of the official version.

135193

Anotácia

Tento dokument špecifikuje požiadavky na vytváranie sektorovo špecifických noriem, ktoré rozširujú ISO/IEC 27001 a dopĺňajú alebo menia ISO/IEC 27002 na podporu špecifického sektora (domény, aplikačnej oblasti alebo trhu).

Tento dokument vysvetľuje, ako:

- zahŕňať požiadavky navyše k požiadavkám v ISO/IEC 27001;
- spresniť alebo vyložiť ktorúkoľvek z požiadaviek ISO/IEC 27001;
- zahŕňať opatrenia okrem tých, ktoré sú uvedené v ISO/IEC 27001: 2013, príloha A a ISO/IEC 27002;
- upraviť ktorýkoľvek z opatrení normy ISO/IEC 27001: 2013, príloha A a ISO/IEC 27002;
- pridať alebo upraviť usmernenie k norme ISO/IEC 27002.

Tento dokument špecifikuje, že dodatočné alebo spresnené požiadavky nerušia platnosť požiadaviek v ISO/IEC 27001.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27001 prijatá ako STN EN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001) (36 9789)

ISO/IEC 27002 prijatá ako STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002) (36 9784)

Vypracovanie slovenskej technickej normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27009:2016), which has been technically revised.

The main changes compared to the previous edition are as follows:

- the scope has been updated to more clearly reflect the content of this document;
- former Annex A has been divided into Annexes A and B;
- Annex C has been created.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements

1 Scope

This document specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001, and complement or amend ISO/IEC 27002 to support a specific sector (domain, application area or market).

This document explains how to:

— include requirements in addition to those in ISO/IEC 27001,

— refine or interpret any of the ISO/IEC 27001 requirements,

— include controls in addition to those of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,

— modify any of the controls of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,

— add guidance to or modify the guidance of ISO/IEC 27002.

This document specifies that additional or refined requirements do not invalidate the requirements in ISO/IEC 27001.

This document is applicable to those involved in producing sector-specific standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirement of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*