ICS 03.100.70; 35.030 SLOVENSKÁ TECHNICKÁ NORMA Júl 2023

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Systémy manažérstva informačnej bezpečnosti Požiadavky**	**STN ISO/IEC 27001** 97 4171

Information security, cybersecurity and privacy protection
Information security management systems
Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée
Systèmes de management de la sécurité de l'information
Exigences

Informationssicherheit, Cybersicherheit und Datenschutz
Informationssicherheitsmanagementsysteme
Anforderungen

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27001: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27001 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27001: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27001 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN EN ISO/IEC 27001 z februára 2019.

136906

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) (97 4170)

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Lenka Gondová, Mgr. Natália Bosnyaková, SynCo s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Systém manažérstva informačnej bezpečnosti
Požiadavky

ISO/IEC 27001
Tretie vydanie
2022-10

ICS 03.100.70; 35.030

Obsah

Contents

Prehovor

ISO (Medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) tvoria špecializovaný systém celosvetovej normalizácie. Národné orgány, ktoré sú členmi ISO alebo IEC, zúčastňujú na tvorbe medzinárodných noriem prostredníctvom technických komisií zriadených týmito organizáciami pre jednotlivé oblasti technickej činnosti. Technické komisie ISO a IEC vzájomne spolupracujú v oblasti spoločného záujmu. S ISO a IEC spolupracujú aj iné medzinárodné vládne alebo mimovládne organizácie.

Postupy použité pri tvorbe tohto dokumentu, ako aj tie, ktoré sú určené na jeho ďalšie udržiavanie, sú opísané v smernici ISO/IEC, Časť 1. Do úvahy sa majú zobrať najmä rozdielne kritériá schvaľovania pri rôznych typoch dokumentov ISO. Tento dokument bol vypracovaný podľa edičných pravidiel smernice ISO/IEC, Časť 2 (pozri www.iso.org/directives alebo www.iec.ch/members_experts/ refdocs).

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. ISO a IEC nezodpovedajú za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv. Podrobnosti o akýchkoľvek patentových právach identifikovaných počas tvorby dokumentu sú uvedené v úvode dokumentu a/alebo v zozname vyhlásení o patentoch ISO (pozri www.iso.org/ patents) alebo v zozname prijatých patentových vyhlásení IEC (pozri https://patents.iec.ch).

Akýkoľvek obchodný názov použitý v tomto dokumente slúži len na informáciu pre používateľa a neznamená jeho schválenie.

Vysvetlenie dobrovoľnej podstaty noriem, význam špecifických termínov a výrazov týkajúcich sa posudzovania zhody, ako aj informácie o väzbe ISO na princípy Svetovej obchodnej organizácie (WTO) uplatňované pri odstraňovaní technických prekážok obchodu (TBT) pozri na www.iso.org/iso/foreword.html. V časti IEC si pozrite www.iec.ch/understanding-standards.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1, Informačné technológie, Podvýbor SC 27, Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia.

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.

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 document 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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of 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. In the IEC, see www.iec.ch/understanding-standards.

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

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27001: 2013), ktoré sa technicky zrevidovalo. Zahŕňa aj technické opravy ISO/IEC 27001: 2013/Cor 1: 2014 a ISO/IEC 27001: 2013/Cor 2: 2015.

Hlavné zmeny sú tieto:

– text bol zosúladený s harmonizovanou štruktúrou noriem systému manažérstva a normou ISO/IEC 27002: 2022.

Akákoľvek spätná väzba alebo otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľa. Úplný zoznam týchto orgánov nájdete na adrese www.iso.org/members.html a www.iec.ch/national-committees.

This third edition cancels and replaces the second edition (ISO/IEC 27001: 2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001: 2013/Cor 1: 2014 and ISO/IEC 27001: 2013/Cor 2: 2015.

The main changes are as follows:

– the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002: 2022.

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 and www.iec.ch/national-committees.

Úvod

0.1 Všeobecne

Tento dokument bol vypracovaný s cieľom poskytnúť požiadavky na stanovenie, implementáciu, udržiavanie a trvalé zlepšovanie systému manažérstva informačnej bezpečnosti. Prijatie systému manažérstva informačnej bezpečnosti je pre organizáciu strategickým rozhodnutím. Vytvorenie a implementáciu systému manažérstva informačnej bezpečnosti organizácie ovplyvňujú potreby a ciele organizácie, bezpečnostné požiadavky, implementované organizačné procesy a veľkosť a štruktúra organizácie. Očakáva sa, že v priebehu času sa všetky tieto ovplyvňujúce faktory budú meniť.

Systém manažérstva informačnej bezpečnosti chráni dôvernosť, integritu a dostupnosť informácií uplatnením procesu riadenia rizík a poskytnutím dôvery zainteresovaným stranám, že riziká sú dostatočne riadené.

Je dôležité, že systém manažérstva informačnej bezpečnosti je súčasťou procesov organizácie a všetkých manažérskych štruktúr a integrovaný do nich. Informačná bezpečnosť je dôležitá pri navrhovaní procesov, informačných systémov a opatrení v organizácii. Očakáva sa, že implementácia systému manažérstva informačnej bezpečnosti bude škálovateľná v závislosti od potrieb organizácie.

Tento dokument sa môže použiť interne, alebo treťou stranou na posúdenie schopnosti organizácie plniť vlastné požiadavky na informačnú bezpečnosť.

Poradie, v ktorom sa požiadavky uvádzajú v tomto dokumente, neznamená poradie ich dôležitosti alebo neurčuje poradie, v akom by sa mali implementovať. Tieto položky sú číslované len z dôvodu referencií.

Norma ISO/IEC 27000 opisuje prehľad a slovník používaný systémom manažérstva informačnej bezpečnosti, odkazuje na ďalšie normy súboru noriem pre systém manažérstva informačnej bezpečnosti (vrátane noriem ISO/IEC 27003[2] ISO/IEC 27004[3] a ISO/IEC 27005[4]), súvisiace termíny a definície.

Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Kompatibilita s inými normami systémov manažérstva

Tento dokument zavádza štruktúru na všeobecnej úrovni, rovnaké názvy kapitol, rovnaký text, bežné výrazy a základné definície, ako ich definuje príloha SL Nariadenia ISO/IEC, Časť 1, upravený doplnok ISO, a preto udržiava kompatibilitu s inými normami systémov manažérstva, ktoré sa prijali v prílohe SL.

Všeobecný prístup, ktorý sa definuje v prílohe SL je užitočný pre také organizácie, ktoré sa rozhodnú implementovať jeden systém manažérstva, ktorý spĺňa požiadavky dvoch alebo viacerých noriem systémov manažérstva.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

1 Predmet normy

Tento dokument špecifikuje požiadavky na stanovenie, implementáciu, udržiavanie a trvalé zlepšovanie systému manažérstva informačnej bezpečnosti v kontexte organizácie. Tento dokument obsahuje aj požiadavky na posúdenie a ošetrenie rizík informačnej bezpečnosti prispôsobených potrebám organizácie. Požiadavky vymedzené v tomto dokumente sú všeobecné a sú určené pre všetky organizácie bez ohľadu na typ, veľkosť alebo povahu organizácie. Nesplnenie niektorej z požiadaviek vymenovaných v kapitolách 4 až 10 nie je akceptovateľné, ak organizácia deklaruje dosiahnutie zhody s týmto dokumentom.

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazov sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Prehľad a slovník.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.