

STN	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Systémy manažérstva informačnej bezpečnosti Požiadavky (ISO/IEC 27001: 2022)	STN EN 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 európskej normy EN ISO/IEC 27001: 2023.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27001 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27001: 2023.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27001 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27001 z júla 2023 v celom rozsahu.

137505

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2023
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii
v znení neskorších predpisov.

Národný predhovor

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. Druhé vydanie ISO/IEC 27001: 2013 bolo v sústave STN implementované vo februári 2019 ako STN EN ISO/IEC 27001.

Hlavné zmeny tohto vydania sú tieto:

- text bol zosúladený s harmonizovanou štruktúrou noriem systému manažérstva a normou ISO/IEC 27001: 2022.

Upozornenie k vydaniu STN EN ISO/IEC 27001

Text STN EN ISO/IEC 27001 z októbra 2023 je **identický** s STN ISO/IEC 27001 z júla 2023. Ide len o zmenu označenia z STN ISO/IEC 27001 na **STN EN ISO/IEC 27001**, pridanie európskej titulnej strany a európskeho predhovoru, a to z dôvodu, že norma bola prevzatá technickou komisiou CEN-CENELEC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov“.

Normatívne referenčné dokumenty

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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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
Systémy manažérstva informačnej bezpečnosti
Požiadavky
(ISO/IEC 27001: 2022)

Information security, cybersecurity and privacy protection
 Information security management systems
 Requirements
 (ISO/IEC 27001: 2022)

Sécurité de l'information, cybersécurité
 et protection de la vie privée
 Systèmes de management de la sécurité
 de l'information
 Exigences (ISO/IEC 27001: 2022)

Informationssicherheit, Cybersicherheit und
 Datenschutz
 Informationssicherheitsmanagementsysteme
 Anforderungen
 (ISO/IEC 27001: 2022)

Túto európsku normu schválil CEN 23. júla 2023.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN a CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Maly, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
 European Committee for Standardization
 Comité Européen de Normalisation
 Europäisches Komitee für Normung

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
 European Committee for Electrotechnical Standardization
 Comité Européen de Normalisation Electrotechnique
 Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Obsah

Európsky predhovor	5
Úvod	7
1 Predmet	8
2 Normatívne odkazy.....	8
3 Termíny a definície	9
4 Organizácia a jej súvislosti.....	9
4.1 Pochopenie organizácie a jej súvislostí	9
4.2 Pochopenie potrieb a očakávaní zainteresovaných strán	9
4.3 Vymedzenie predmetu systému manažérstva informačnej bezpečnosti.....	9
4.4 Systém manažérstva informačnej bezpečnosti.....	10
5 Vodcovstvo	10
5.1 Vodcovstvo a záväzok.....	10
5.2 Politika	11
5.3 Roly, zodpovednosti a právomoci v organizácii	11
6 Plánovanie	12
6.1 Opatrenia na zvládnutie rizík a príležitostí	12
6.1.1 Všeobecne	12
6.1.2 Posúdenie rizík informačnej bezpečnosti.....	12
6.1.3 Ošetrovanie rizík informačnej bezpečnosti.....	13
6.2 Ciele informačnej bezpečnosti a plánovanie ich splnenia	14
6.3 Plánovanie zmien.....	15
7 Podpora.....	15
7.1 Zdroje.....	15
7.2 Kompetentnosť.....	15
7.3 Povedomie	15
7.4 Komunikácia	16

Contents

European foreword	5
Introduction	7
1 Scope	8
2 Normative references.....	8
3 Terms and definitions	9
4 Context of the organization.....	9
4.1 Understanding the organization and its context	9
4.2 Understanding the needs and expectations of interested parties.....	9
4.3 Determining the scope of the information security management system.....	9
4.4 Information security management system	10
5 Leadership	10
5.1 Leadership and commitment	10
5.2 Policy	11
5.3 Organizational roles, responsibilities and authorities	11
6 Planning	12
6.1 Actions to address risks and opportunities.....	12
6.1.1 General.....	12
6.1.2 Information security risk assessment.....	12
6.1.3 Information security risk treatment.....	13
6.2 Information security objectives and planning to achieve them.....	14
6.3 Planning of changes.....	15
7 Support.....	15
7.1 Resources	15
7.2 Competence	15
7.3 Awareness.....	15
7.4 Communication.....	16

7.5	Zdokumentované informácie.....	16	7.5	Documented information	16
7.5.1	Všeobecne	16	7.5.1	General	16
7.5.2	Tvorba a aktualizácia	16	7.5.2	Creating and updating.....	16
7.5.3	Riadenie zdokumentovaných informácií.....	17	7.5.3	Control of documented information.....	17
8	Prevádzka	17	8	Operation.....	17
8.1	Plánovanie a riadenie prevádzky	17	8.1	Operational planning and control.....	17
8.2	Posúdenie rizík informačnej bezpečnosti	18	8.2	Information security risk assessment.....	18
8.3	Ošetrovanie rizík informačnej bezpečnosti	18	8.3	Information security risk treatment.....	18
9	Hodnotenie výkonnosti.....	18	9	Performance evaluation.....	18
9.1	Monitorovanie, meranie, analýza a hodnotenie	18	9.1	Monitoring, measurement, analysis and evaluation.....	18
9.2	Interný audit.....	19	9.2	Internal audit.....	19
9.2.1	Všeobecne	19	9.2.1	General	19
9.2.2	Program interného auditu	19	9.2.2	Internal audit programme.....	19
9.3	Preskúmanie manažmentom	20	9.3	Management review	20
9.3.1	Všeobecne.....	20	9.3.1	General	20
9.3.2	Vstupy do preskúmania manažmentom	20	9.3.2	Management review inputs	20
9.3.3	Výsledky preskúmania manažmentom	20	9.3.3	Management review results	20
10	Zlepšovanie	21	10	Improvement.....	21
10.1	Trvalé zlepšovanie	21	10.1	Continual improvement	21
10.2	Nezhoda a nápravné opatrenie.....	21	10.2	Nonconformity and corrective action.....	21
Príloha A	(normatívna) – Odkaz na opatrenia informačnej bezpečnosti.....	22	Annex A	(normative) – Information security controls reference.....	22
Literatúra		41	Bibliography		41

Európsky predhovor

Tento dokument (ISO/IEC 27001: 2022) vypracovala technická komisia ISO/IEC JTC 1 „Informačné technológie“ medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27001: 2023 technickou komisiou CEN-CENELEC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov“, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskoršie do januára 2024 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskoršie do januára 2024.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN-CENELEC nezodpovedá za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Tento dokument nahrádza EN ISO/IEC 27001: 2017.

Akákoľvek spätná väzba a otázky k tejto európskej norme majú byť adresované národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov možno nájsť na webovej stránke CEN a CENELEC.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cyprus, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunská, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédsko, Talianska a Turecko.

Oznámenie o schválení

Text ISO/IEC 27001: 2022 chválil CEN-CENELEC ako EN ISO/IEC 27001: 2023 bez akýchkoľvek modifikácií.

European foreword

The text of ISO/IEC 27001:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27001:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2024, and conflicting national standards shall be withdrawn at the latest by January 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27001: 2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27001: 2022 has been approved by CEN-CENELEC as EN ISO/IEC 27001: 2023 without any modification.

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.

1 Predmet

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 ošetrovanie rizík informačnej bezpečnosti prispôbených 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.

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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

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

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 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 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.

3 Termíny a definície

Na účely tohto dokumentu platia termíny a definície uvedené v ISO/IEC 27000.

ISO a IEC udržiavajú terminologické databázy na používanie v normalizácii na nasledujúcich adresách:

- ISO online browsing platform: dostupné na <https://www.iso.org/obp>;
- IEC Electropedia: dostupné na <http://www.electropedia.org/>.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>;
- IEC Electropedia: available at <http://www.electropedia.org/>.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN