ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030 **Říjen 2023**

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

ČSN EN ISO/IEC 27001

36 9797

idt ISO/IEC 27001:2022

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

Sécurité de l,information, cybersécurité et protection de la vie privée – Systemes de management de la sécurité
de l,information – Exigences

Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen

Tato norma je českou verzí evropské normy EN ISO/IEC 27001:2023. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27001:2023. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO/IEC 27001 (36 9797) ze září 2014.

Národní předmluva

Změny proti předchozí normě

Název normy byl změněn. Text byl uveden do souladu s harmonizovanou strukturou norem systému mana-
gementu a s ISO/IEC 27002:2022.

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Souvisící ČSN

ČSN EN ISO/IEC 27002:2023 (36 9798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

ČSN ISO/IEC 27003 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

ČSN ISO 31000:2018 (01 0351) Management rizik – Směrnice

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Vypracování normy

Zpracovatel: Česká agentura pro standardizaci, IČO 06578705

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

EVROPSKÁ NORMA EN ISO/IEC 27001
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Červenec 2023

ICS 03.100.70; 35.030 Nahrazuje
EN ISO/IEC 27001:2017

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí –
Systémy managementu informační bezpečnosti – Požadavky
(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 – Systemes de management de la sécurité de l,information – Exigences (ISO/IEC 27001:2022)	Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022)

Tato evropská norma byla schválena CEN dne 2023-07-23.

Členové CEN a CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy. Aktualizované
seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru
CEN-CENELEC nebo u kteréhokoliv člena CEN a CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém
jiném jazyce přeložená členem CEN a CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Řídicí centrum CEN-CENELEC
Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO/IEC 27001:2023 E

Členy CEN a CENELEC jsou národní normalizační orgány a národní elektrotechnické komise Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky
Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Evropská předmluva

Text ISO/IEC 27001:2022 vypracovala technická komise ISO/IEC JTC 1 *Informační technologie* Mezinárodní organizace pro normalizaci (ISO) a byl převzat jako EN ISO/IEC 27001:2023 technickou komisí CEN-CENELEC/JTC 13 *Kybernetická bezpečnost a ochrana dat*, jejímž sekretariátem je DIN.

Této evropské normě je nutno nejpozději do ledna 2024 udělit status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do ledna 2024.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv.
CEN-CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument nahrazuje EN ISO/IEC 27001:2017.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CEN a CENELEC.

Podle vnitřních předpisů CEN-CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Oznámení o schválení

Text ISO/IEC 27001:2022 byl schválen CEN-CENELEC jako EN ISO/IEC 27001:2023 bez jakýchkoliv modifikací.

Obsah

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives nebo www.iec.ch/members_experts/refdocs).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržených IEC (viz https://patents.iec.ch).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí.*

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27001:2013), které bylo technicky zrevidováno. To zahrnuje také technické opravy ISO/IEC 27001:2013/Cor. 1:2014 a ISO/IEC 27001:2013/Cor. 2:2015.

Hlavní změny jsou:

– text byl uveden do souladu s harmonizovanou strukturou norem systému managementu a ISO/IEC 27002:2022.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html a www.iec.ch/national-committees.

Úvod

0.1 Obecně

Tento dokument byl vypracován za účelem ustavení, zavedení, udržování a neustálého zlepšování systému mana-
gementu informační bezpečnosti. Přijetí systému managementu informační bezpečnosti je pro organizaci strategickým rozhodnutím. Ustavení a zavedení systému managementu informační bezpečnosti organizace jsou ovlivněny potřebami a cíli organizace, požadavky na bezpečnost, používanými procesy a velikostí a strukturou organizace. Všechny tyto ovlivňující faktory se pravděpodobně budou v čase měnit.

Systém managementu informační bezpečnosti zachovává důvěrnost, integritu a dostupnost informací aplikováním procesu managementu rizik a dává jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena.

Je důležité, aby byl systém managementu informační bezpečnosti součástí procesů a celkové struktury mana-
gementu organizace, a aby byla informační bezpečnost zohledněna při návrhu procesů, informačních systémů a opatření. Očekává se, že zavedení systému managementu informační bezpečnosti bude nastaveno v souladu s potřebami organizace.

Tento dokument může být použit interními a externími stranami k posuzování schopnosti organizace splnit její vlastní požadavky informační bezpečnosti.

Pořadí, ve kterém jsou v tomto dokumentu požadavky uvedeny, neodráží jejich důležitost ani nenaznačuje pořadí, ve kterém mají být zavedeny. Položky seznamu jsou seřazeny pouze pro referenční účely.

ISO/IEC 27000 popisuje přehled a slovník systémů managementu informační bezpečnosti, a odkazuje na řadu norem systému managementu informační bezpečnosti (včetně ISO/IEC 27003[2], ISO/IEC 27004[3] a ISO/IEC 27005[4]) se souvisejícími termíny a definicemi.

0.2 Kompatibilita s jinými normami systémů managementu

Tento dokument používá základní strukturu, identické názvy článků, identický text, společné termíny a hlavní definice vymezené v příloze SL směrnic ISO/IEC, část 1, konsolidovaný dodatek ISO, a proto zachovává kompatibilitu s ostatními normami systému managementu, které přijaly tuto přílohu SL.

Tento společný přístup podle přílohy SL bude užitečný pro ty organizace, které se rozhodnou provozovat jediný systém managementu, který splňuje požadavky dvou a více norem systému managementu.

1 Předmět normy

Tento dokument specifikuje požadavky na ustavení, zavedení, udržování a neustálé zlepšování systému mana-
gementu informační bezpečnosti v rámci kontextu organizace. Tento dokument také zahrnuje požadavky na posu-
zování a ošetření rizik informační bezpečnosti, přizpůsobené potřebám organizace. Požadavky tohoto dokumentu jsou obecné a jsou určené pro použití ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků specifikovaných v kapitolách 4 až 10 je nepřijatelné, pokud organizace prohlašuje shodu s tímto dokumentem.