ČESKÁ SPOLEČNOST PRO JAKOST

ČESKÁ AGENTURA PRO STANDARDIZACI

Komentované vydání normy

ČSN EN ISO/IEC 27001:2023

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

KOMENTOVANÉ VYDÁNÍ NORMY ČSN EN ISO/IEC 27001:2023

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

Autor:
Ing. Ondřej Salák

Recenzent:
Ing. Petr Koten

Publikace obsahuje platné znění normy

Česká společnost pro jakost
Praha 2025

Národní předmluva

Změny proti předchozí normě

Název normy byl změněn. Text byl uveden do souladu s harmonizovanou strukturou norem systému managementu 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
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

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 – Systèmes 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.

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.

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

Ref. č. EN ISO/IEC 27001:2023 E

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.

Komentář autora

Tento komentář k normě **ISO/IEC 27001** je vytvořen jako **průvodce** pro všechny, kteří implementují nebo spravují systém managementu informační bezpečnosti (dále též systém ISMS). Komentář je navržen tak, aby umožnil uživatelům vybrat relevantní části, které potřebují řešit, přičemž poskytuje jasné praktické pokyny pro jednotlivé oblasti normy. Struktura komentářů je navržena tak, aby co nejvíce usnadnila orientaci a implementaci opatření na základě skutečných potřeb a kontextu organizace.

Struktura komentářů:

Komentáře jsou rozděleny do několika sekcí, které mají za cíl **zjednodušit** orientaci v normě a implementaci jednotlivých požadavků. V tomto komentovaném vydání je možno se setkat s následujícími typy sekcí (komentářů):

1. **O čem to je?**: Tato sekce stručně představuje klíčové téma, kterým se konkrétní článek normy zabývá. Je to rychlý úvod, který čtenáři poskytne základní porozumění bez potřeby hlubšího studia celé normy.
2. **Jak na to**: V této sekci jsou poskytnuty **praktické kroky** a doporučení, jak přistupovat k implementaci požadavků normy ISO/IEC 27001. Zde se čerpá z osvědčené praxe a z normy **ISO/IEC 27002**, která detailněji popisuje jednotlivá bezpečnostní opatření.
3. **Takto ne**: Upozorňuje na **nejčastější chyby**, kterým by se organizace měla vyhnout při implementaci. Sekce zahrnuje varování před potenciálními problémy, které mohou nastat při nesprávné aplikaci vhodných opatření.
4. **Možná integrace**: Tato část zkoumá, jak lze dané požadavky normy **integrovat s jinými standardy pro systémy managementu**, jako je **ISO 9001** nebo **ISO 14001**, čímž se zjednodušuje správa různých systémů managementu v organizaci.

5. **Další normy/legislativa**: V této části jsou u vybraných opatření diskutovány specifické požadavky **jiných legislativních nebo normativních dokumentů**.

Příloha A: Tento materiál zahrnuje komentáře jen k těm opatřením z přílohy A, která upřesňují konkrétní požadavky z kapitol **4–10** normy. Tato opatření pomáhají organizaci správně implementovat procesy jako je řízení rizik, plánování bezpečnosti a neustálé zlepšování systému ISMS. Všechna další opatření, která jsou v Příloze A uvedena, jsou podrobně popsána v normě **ISO/IEC 27002 a** zde nejsou komentována. Pro efektivní implementaci systému ISMS tedy doporučujeme si i normu ISO/IEC 27002 pořídit.

Úvod

0.1 Obecně

Tento dokument byl vypracován za účelem ustavení, zavedení, udržování a neustálého zlepšování systému managementu 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 managementu 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.

Komentář autora

Systém managementu informační bezpečnosti (**ISMS**) představuje pro organizace nezbytný nástroj, který umožňuje řídit a minimalizovat rizika spojená s ochranou informací. V době, kdy kybernetické útoky a bezpečnostní incidenty exponenciálně narůstají – ať už se jedná o ransomwarové útoky, úniky citlivých dat nebo pokusy o narušení kritických systémů – je pro organizace naprosto zásadní, aby zavedly robustní a systematický přístup k bezpečnosti. Mnoho organizací se dnes ocitá pod neustálým tlakem, kdy musí chránit nejen své vlastní informace, ale také data svých zákazníků, obchodních partnerů a dodavatelského řetězce. Porušení důvěrnosti nebo narušení provozu může mít pro organizaci katastrofální důsledky, od ztráty důvěry klientů až po vysoké pokuty ze strany regulačních orgánů nebo ztrátu obchodních příležitostí.

Implementace systému ISMS podle normy **ISO/IEC 27001** umožňuje organizacím vytvořit strukturovaný rámec, který nejen zajišťuje ochranu citlivých informací, ale také stanovuje jasný proces pro identifikaci, hodnocení a ošetření rizik informační bezpečnosti. Tento standardizovaný přístup zajišťuje, že přijatá bezpečnostní opatření jsou konzistentní, prověřená a pravidelně revidovaná, což organizaci umožňuje reagovat na nové hrozby efektivně a včas. Klíčovou výhodou je také to, že tento systém podporuje **neustálé zlepšování**, což znamená, že bezpečnost není jednorázovým projektem, ale neustálým procesem, který se přizpůsobuje vývoji technologií a změnám v prostředí.

Jedním z hlavních přínosů systému ISMS je možnost **standardizace bezpečnostních procesů**, což přináší nejen vyšší úroveň ochrany, ale také snižuje provozní náklady a zefektivňuje správu bezpečnosti. Organizace, které zavádějí systém ISMS, musí jasně definovat odpovědnosti a kompetence jednotlivých pracovníků, což zlepšuje vnitřní komunikaci a spolupráci napříč odděleními. Systém také umožňuje lépe řídit zdroje, přičemž eliminuje duplicitní nebo neefektivní činnosti.

Systém ISMS však nepřináší jen **interní výhody**, ale také výrazně posiluje **externí důvěryhodnost** organizace. Certifikace podle ISO/IEC 27001 se stává stále častěji podmínkou pro obchodní vztahy, účast ve veřejných zakázkách nebo přístup na regulované trhy. Zákazníci, partneři a investoři stále více požadují, aby jejich dodavatelé a obchodní partneři prokazovali schopnost chránit informace a certifikace je jasným důkazem o plnění těchto požadavků. Organizace se systémem ISMS jsou proto vnímány jako spolehlivější, lépe řízené a odpovědné vůči svým závazkům.

Navíc systém ISMS poskytuje **konkurenční výhodu**. V dnešní době, kdy jsou informace jedním z nejcennějších aktiv každé organizace, se bezpečnost stává klíčovým faktorem, který rozhoduje o úspěchu či neúspěchu na trhu. Subjekty, které prokazatelně chrání své informace a informace svých zákazníků, jsou lépe připraveny čelit bezpečnostním výzvám, což jim poskytuje náskok před konkurencí. Certifikace také otevírá dveře k novým obchodním příležitostem, protože mnoho velkých korporací a institucí vyžaduje vysoké standardy bezpečnosti u svých dodavatelů.

Z dlouhodobého hlediska přináší systém ISMS **úsporu nákladů**. Investice do preventivních bezpečnostních opatření je mnohem nižší než náklady spojené s řešením bezpečnostních incidentů, jako jsou náklady na obnovu dat, ztráta důvěry zákazníků nebo pokuty od regulačních orgánů. Systém managementu informační bezpečnosti pomáhá organizacím být proaktivní, identifikovat potenciální rizika včas a minimalizovat jejich dopad na provoz a obchodní výsledky. V konečném důsledku tedy systém ISMS nejen chrání organizaci, ale také zajišťuje její **dlouhodobou odolnost** a schopnost adaptovat se na stále měnící se hrozby v digitálním světě.

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.

Komentář autora

Integrace různých systémů managementu je výrazně usnadněna prostřednictvím **Annexu SL**. Annex SL definuje jednotnou strukturu pro všechny normy ISO pro systémy managementu, což znamená, že základní prvky, jako jsou termíny, číslování kapitol a procesní požadavky, jsou ve všech těchto normách shodné. To platí nejen pro normu **ISO/IEC 27001** (systém managementu informační bezpečnosti), ale i pro další normy, jako je **ISO 9001** (systém managementu kvality) nebo **ISO 14001** (systém environmentálního managementu) a další.

Tato **harmonizovaná struktura** usnadňuje integraci různých systémů managementu v rámci jedné organizace, protože sdílí společné principy řízení rizik, neustálého zlepšování a hodnocení výkonnosti. Organizace tak mohou efektivněji spravovat více systémů managementu, aniž by musely vyvíjet zcela samostatné procesy pro každý z nich. V praxi to znamená, že organizace může například snadno integrovat **interní audity** pro různé systémy, zavést jednotné postupy řízení dokumentace nebo efektivně koordinovat zdroje a odpovědnosti napříč odděleními. Tato unifikace zvyšuje efektivitu a snižuje náklady, což je jedním z hlavních důvodů, proč se stále více organizací rozhoduje pro integraci svých systémů managementu na základě struktury stanovené Annexem SL.