ČESKÁ TECHNICKÁ NORMA

ICS 03.100.01; 03.100.70 **Duben 2023**

Bezpečnost a odolnost – Systémy managementu bezpečnosti – Požadavky

ČSN ISO 28000

01 0381

Security and resilience – Security management systems – Requirements

Tato norma je českou verzí mezinárodní normy ISO 28000:2022. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 28000:2022. 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 ISO 28000 (01 0381) z června 2010.

Národní předmluva

Změny proti předchozí normě

Změny proti normě ISO 28000:2007 jsou uvedeny v Předmluvě.

Informace o citovaných dokumentech

ISO 22300 zavedena v ČSN EN ISO 22300 (01 2301) Bezpečnost a odolnost – Slovník

Souvisící ČSN

ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

ČSN EN ISO 14001 (01 0901) Systémy environmentálního managementu – Požadavky s návodem pro použití

ČSN EN ISO 19011 (01 0330) Směrnice pro auditování systémů managementu

ČSN EN ISO 22301 (01 2306) Bezpečnost a odolnost – Systémy managementu kontinuity podnikání – Požadavky

ČSN EN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení

bezpečnosti informací – Požadavky

ČSN ISO 31000 (01 0351) Management rizik – Směrnice

ČSN ISO 45001 (01 0801) Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky s návodem k použití

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: Asociace technických bezpečnostních služeb Grémium Alarm z. s. – Centrum technické normalizace pro bezpečnostní služby, IČO 63839911, Ing. Vladimír Šimek; spolupráce: Ing. Martin Škutek

Pracovník České agentury pro standardizaci: Mgr. Anna Mezuliáníková

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.

MEZINÁRODNÍ NORMA

Bezpečnost a odolnost
Systémy managementu bezpečnosti – Požadavky

ISO 28000
Druhé vydání
2022-03

ICS 03.100.01; 03.100.70

Obsah

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů
(členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

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 ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2. (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou 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).

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), jsou uvedeny na tomto odkazu URL www.iso.org/iso/foreword.html.

Tento dokument vypracovala technická komise ISO/TC 292 *Bezpečnost a odolnost*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO 28000:2007), které bylo technicky revidováno, ale zachovává stávající požadavky, aby byla zajištěna kontinuita pro organizace používající předchozí vydání. Hlavní změny jsou tyto:

- do kapitoly 4 byla doplněna doporučení týkající se zásad, aby byla zajištěna lepší koordinace s ISO 31000;
- do kapitoly 8 byla doplněna doporučení pro lepší soulad s ISO 22301, což usnadňuje integraci včetně:
    - bezpečnostních strategií, postupů, procesů a řešení;
    - bezpečnostních plánů.

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

Úvod

Většina organizací se potýká s rostoucí nejistotou a nestálostí bezpečnostního prostředí. V důsledku toho se potýkají s bezpečnostními problémy, které mají dopad na jejich cíle, které chtějí systematicky řešit v rámci svého systému managementu. Formální přístup k managementu bezpečnosti může přímo přispět k obchodní způsobilosti a důvěryhodnosti organizace.

Tento dokument specifikuje požadavky na systém managementu bezpečnosti, včetně těch aspektů, které jsou rozhodující pro zajištění bezpečnosti dodavatelského řetězce. Vyžaduje se, aby organizace:

- posoudila bezpečnostní prostředí, ve kterém působí, včetně svého dodavatelského řetězce (včetně závislostí a vzájemných vazeb);
- zjistila, zda jsou zavedena odpovídající bezpečnostní opatření k účinnému řízení rizik souvisejících s bezpečností;
- řídila dodržování zákonných, regulačních a dobrovolných povinností, ke kterým se zavázala;
- sladila bezpečnostní procesy a kontroly, včetně příslušných předcházejících a následujících procesů a kontrol dodavatelského řetězce, aby byly splněny cíle organizace.

Management bezpečnosti je spojen s mnoha aspekty obchodního managementu. Tyto aspekty zahrnují všechny činnosti řízené nebo ovlivňované organizacemi, mimo jiné i ty, které mají dopad na dodavatelský řetězec. Měly by se brát v úvahu všechny činnosti, funkce a operace, které mají dopad na management bezpečnosti organizace, včetně (ale nejen) jejího dodavatelského řetězce.

Pokud jde o dodavatelský řetězec, je třeba vzít v úvahu, že dodavatelské řetězce mají dynamickou povahu. Proto smí některé organizace, které řídí více dodavatelských řetězců, požadovat, aby jejich poskytovatelé splňovali související bezpečnostní normy jako podmínku pro zařazení do tohoto dodavatelského řetězce, aby splnili požadavky na management bezpečnosti.

Tento dokument uplatňuje model Plánuj – Dělej – Kontroluj – Jednej (PDCA) při plánování, stanovení, zavedení, provozování, monitorování, přezkoumávání, udržování a neustálém zlepšování účinnosti systému managementu bezpečnosti organizace, viz tabulka 1 a obrázek 1.

Tabulka 1 – Vysvětlení PDCA modelu

Plánuj (stanov)	Stanovení bezpečnostní politiky, cílů, cílových hodnot, kontrolních mechanismů, procesů a postupů týkajících se zlepšování bezpečnosti, aby bylo možné dosáhnout výsledků, které jsou v souladu s celkovými zásadami a cíli organizace.
Dělej (zaváděj a provozuj)	Zavedení a provozování bezpečnostní politiky, kontrolních mechanismů, procesů a postupů.
Kontroluj (monitoruj a přezkoumávej)	Monitorování a přezkoumávání výkonnosti v porovnání s bezpečnostní politikou a cíli, podávat zprávy o výsledcích vedení k přezkoumání a určovat a schvalovat opatření k nápravě a zlepšení.
Jednej (udržuj a zlepšuj)	Udržování a zlepšování systému managementu bezpečnosti přijímáním nápravných opatření na základě výsledků přezkoumání managementu a přehodnocením rozsahu systému managementu bezpečnosti a bezpečnostní politiky a cílů.

Obrázek 1 – PDCA model aplikovaný na systém managementu bezpečnosti

Tím je zajištěna určitá míra konzistence s ostatními normami systémů managementu, jako jsou ISO 9001,
ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 atd., což podporuje konzistentní a integrované zavádění a provozování souvisejících systémů managementu.

U organizací, které si to přejí, smí být shoda systému managementu bezpečnosti s tímto dokumentem ověřena prostřednictvím externího nebo interního auditu.

1 Předmět normy

Tento dokument specifikuje požadavky na systém managementu bezpečnosti, včetně aspektů týkajících se dodavatelského řetězce.

Tento dokument je použitelný pro organizace všech typů a velikostí (např. komerční podniky, vládní nebo jiné veřejné agentury a neziskové organizace), které hodlají stanovit, zavést, udržovat a zlepšovat systém managementu bezpečnosti. Poskytuje ucelený a společný přístup a není odvětvově specifický.

Tento dokument může být používán po celou dobu existence organizace a může být aplikován na jakoukoliv činnost, interní i externí, na všech úrovních.