ČESKÁ TECHNICKÁ NORMA

ICS 01.040.35; 03.100.70; 35.030 **Červen 2020**

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN ISO/IEC 27000

36 9790

idt ISO/IEC 27000:2018

Information technology – Security techniques – Information security management systems – Overview and vocabulary

Technologies de l,information – Techniques de sécurité – Systemes de management de la sécurité de l,information – Vue d,ensemble et vocabulaire

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie

Tato norma je českou verzí evropské normy EN ISO/IEC 27000:2020. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27000:2020. 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 27000 (36 9790) z května 2017.

Národní předmluva

Změny proti předchozí normě

Toto páté vydání zařazuje do seznamu řady norem ISMS aktualizované a nově vydané normy.

Souvisící ČSN a TNI

ČSN EN ISO 9000:2016 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN EN ISO/IEC 17021 (01 5257) Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu

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

ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

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/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27006 (36 9790) Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

ČSN ISO/IEC 27007 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN ISO/IEC 27017 (36 9710) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

ČSN ISO/IEC 27018 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

ČSN EN ISO 27799 (98 2021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

TNI 01 0350:2010 (01 0350) Management rizik – Slovník (Pokyn 73)

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit

- překlad anglického termínu „management“ jako „řízení“ s ohledem na jeho preferované používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména normy řady 27XXX;
- překlad anglického termínu „control“ jako „opatření“, „řízení“ nebo „kontrola“ s ohledem na význam v textu normy;
- v případech, kdy jsou u definice převzaté z odkazovaných norem uvedeny dva termíny (nebo více termínů), je první z nich termín preferovaně používaný v IT.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

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 27000
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Únor 2020

ICS 01.040.35; 35.030 Nahrazuje
EN ISO/IEC 27000:2017

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník (ISO/IEC 27000:2018)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018)

Technologies de l,information – Techniques de sécurité – Systemes de management de la sécurité de l,information – Vue d,ensemble et vocabulaire (ISO/IEC 27000:2018)

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018)

Tato evropská norma byla schválena CEN dne 2019-10-20.

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

Evropská předmluva

Text normy ISO/IEC 27000:2018 vypracovala technická komise ISO/IEC JTC 1 *Informační technologie* Mezinárodní organizace pro normalizaci (ISO) a byla převzata jako EN ISO/IEC 27000:2020 technickou komisí CEN/CLC/JTC13 *Kybernetická bezpečnost a ochrana dat*, za jehož sekretariát odpovídá DIN.

Této evropské normě je nutno nejpozději do srpna 2020 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 srpna 2020.

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

Tento dokument nahrazuje EN ISO/IEC 27000:2017.

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 27000:2018 byl schválen CEN jako EN ISO/IEC 27000:2020 bez jakýchkoliv modifikací.

Obsah

Strana

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní 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 norem, významu specifických termínů a výrazů ISO, které se vztahují k posu-
zování 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 společná technická komise ISO/IEC JTC 1 *Informační technologie* subkomise SC 27 *IT Bezpečnostní techniky.*

Toto páté vydání zrušuje a nahrazuje čtvrté vydání (ISO/IEC 27000:2016), které bylo technicky revidováno. Hlavní změny proti předchozímu vydání jsou:

- Úvod byl přeformulován;
- některé termíny a definice byly odstraněny;
- kapitola 3 byla sladěna na vyšší úrovni struktury pro MSS;
- kapitola 5 byla aktualizována, aby reflektovala změny v dotyčných normách;
- přílohy A a B byly vypuštěny.

Úvod

0.1 Přehled

Mezinárodní normy pro systémy řízení poskytují model určený k využití při vytváření a provozování systému řízení. Tento model obsahuje rysy, u kterých experti v daném oboru dosáhli shody, pokud jde o poslední stav mezinárodního vývoje. ISO/IEC JTC 1/SC 27 udržuje komisi expertů, která se věnuje vývoji mezinárodních norem systémů řízení bezpečnosti informací, označovaných také jako řada norem Systém řízení bezpečnosti informací (Information Security Management System (ISMS)).

Organizace mohou použitím řady norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých informačních aktiv zahrnujících finanční informace, duševní vlastnictví a podrobnosti o zaměstnancích nebo infor-
mace, které jim byly svěřeny zákazníky nebo třetími stranami. Tyto normy mohou být také použity pro přípravu na nezávislé posouzení jejich ISMS týkající se ochrany informací.

0.2 Účel tohoto dokumentu

Tato řada norem ISMS zahrnuje normy, které:

a) stanovují požadavky na ISMS a na pracovníky, kteří takové systémy certifikují;

b) poskytují přímou podporu, podrobný návod a/nebo interpretaci pro celkový proces ustavení, implementování, udržování a zlepšování ISMS;

c) se zabývají směrnicemi pro ISMS specifickými pro jednotlivá odvětví;

d) se zabývají posuzováním shody ve vztahu k ISMS.

0.3 Obsah tohoto dokumentu

V tomto dokumentu jsou použity následující slovesné formy:

– „musí“ označuje požadavek;

– „měl by“ označuje doporučení;

– „smí“ označuje dovolení;

– „může“ označuje možnost nebo schopnost.

Informace označené jako „POZNÁMKA“ jsou návodem pro pochopení nebo objasnění připojeného požadavku. „Poznámky k heslu“, použité v kapitole 3, poskytují další informace, které doplňují terminologická data a mohou obsahovat ustanovení související s použitím termínu.

1 Předmět normy

Tento dokument poskytuje přehled systémů řízení bezpečnosti informací (ISMS). Poskytuje také termíny a definice běžně používané v řadě norem ISMS. Tento dokument je použitelný pro všechny typy a velikosti organizací (například pro obchodní podniky, vládní úřady, neziskové organizace).

Termíny a definice poskytnuté v tomto dokumentu:

- obsahují běžně používané termíny a definice v řadě norem ISMS;
- neobsahují všechny termíny a definice použité v řadě norem ISMS; a
- neomezují řadu norem ISMS v definování nových termínů.