ČESKÁ TECHNICKÁ NORMA

ICS 01.040.35; 03.100.70; 35.030

Květen 2017

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

ČSN
EN ISO/IEC 27000

36 9790

idt ISO/IEC 27000:2016

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

Technologies de l,information – Techniques de sécurité – Systemes de gestion de 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 27000:2017. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27000:2017. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27000 (36 9790) z října 2014.

Národní předmluva

Změny proti předchozí normě

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

Souvisící ČSN

ČSN EN ISO/IEC 17021-1 (01 5257) Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky

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

ČSN EN ISO 19011:2012 (01 0330) Směrnice pro auditování systémů managementu

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

ČSN 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 – Směrnice pro implementaci systému řízení bezpečnosti informací

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

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)

ČSN ISO/IEC 15939:2011 (36 9040) Systémové a softwarové inženýrství – Proces měření

ČSN ISO/IEC 20000-1:2012 (36 9074) Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb

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 preferovaně používaný v IT.

V číslování bibliografických zdrojů je v kapitole Bibliografie originálu mezinárodní normy ISO/IEC 27000:2016 pořadové číslo [20] uvedeno dvakrát. Tato chyba je v překladu normy opravena.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

EVROPSKÁ NORMA EN ISO/IEC 27000
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Únor 2017

ICS 01.040.35; 03.100.70; 35.030

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník (ISO/IEC 27000:2016)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2016)

Technologies de l,information – Techniques de sécurité – Systemes de gestion de sécurité de l,information – Vue d,ensemble et vocabulaire (ISO/IEC 27000:2016)

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2016)

Tato evropská norma byla schválena CEN dne 2017-01-26.

Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
Řídicí centrum CEN-CENELEC: Avenue Marnix 17, B-1000 Brusel

Ref. č. EN ISO/IEC 27000:2017 E

Členy CEN a CENELEC jsou národní normalizační orgány Belgie, Bulharska, Bývalé jugoslávské

republiky
Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska,
Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Evropská předmluva

Text normy ISO/IEC 27000:2016 vypracovala technická komise ISO/IEC JTC 1 Informační technologie Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnické komise (IEC) a byla převzata jako EN ISO/IEC 27000:2017.

Této evropské normě je nutno nejpozději do srpna 2017 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 2017.

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

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

Oznámení o schválení

Text ISO/IEC 27000:2016 byl schválen CEN jako EN ISO/IEC 27000:2017 bez jakýchkoliv modifikací.

Obsah

Strana

ISO copyright office
Ch. de Blandonnet 8 · CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

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 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 a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

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 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).

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

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information.

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Toto čtvrté vydání zrušuje a nahrazuje třetí vydání (ISO/IEC 27000:2014), které bylo technicky zrevidováno.

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, 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 informace, 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 Řada norem ISMS

Řada norem ISMS (viz kapitola 4) má pomoci organizacím všech typů a velikostí zavést a provozovat ISMS. Sestává z následujících mezinárodních norem se společným názvem *Informační technologie – Bezpečnostní techniky* (uvedených dále v číselném pořadí):

- ISO/IEC 27000 *Systémy řízení bezpečnosti informací – Přehled a slovník*
- ISO/IEC 27001 *Systémy řízení bezpečnosti informací – Požadavky*
- ISO/IEC 27002 *Soubor postupů pro opatření bezpečnosti informací*
- ISO/IEC 27003 *Směrnice pro implementaci systému řízení bezpečnosti informací*
- ISO/IEC 27004 *Řízení bezpečnosti informací – Měření*
- ISO/IEC 27005 *Řízení rizik bezpečnosti informací*
- ISO/IEC 27006 *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*
- ISO/IEC 27007 *Směrnice pro audit systémů řízení bezpečnosti informací*
- ISO/IEC TR 27008 *Směrnice pro auditory opatření bezpečnosti informací*
- ISO/IEC 27009 *Oborově specifická aplikace ISO/IEC 27001 – Požadavky*
- ISO/IEC 27010 *Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*
- ISO/IEC 27011 *Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*
- ISO/IEC 27013 *Pokyn pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*
- ISO/IEC 27014 *Správa a řízení bezpečnosti informací*

- ISO/IEC TR 27015 *Směrnice pro řízení bezpečnosti informací pro finanční služby*
- ISO/IEC TR 27016 *Řízení bezpečnosti informací – Organizační ekonomika*
- ISO/IEC 27017 *Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002*
- ISO/IEC 27018 *Soubor postupů pro ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII*
- ISO/IEC 27019 *Směrnice pro řízení bezpečnosti informací na základě ISO/IEC 27002 pro systémy řízení procesů specifické pro odvětví energetiky*

POZNÁMKA Společný název „*Informační technologie – Bezpečnostní techniky*“ označuje, že tyto mezinárodní normy byly vypracovány společnou technickou komisí ISO/IEC JTC 1 *Informační technologie,* subkomisí SC 27 *IT Bezpečnostní techniky*.

Mezinárodní normy, které nejsou uvedeny pod tímto společným názvem, ale jsou také součástí řady norem ISMS, jsou uvedeny dále:

- ISO 27799 *Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*

0.3 Účel této mezinárodní normy

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací a definuje související termíny.

POZNÁMKA V Příloze A je objasněno, jak jsou v řadě norem ISMS použity slovesné tvary k vyjádření požadavků a/nebo pokynů.

Řada norem ISMS zahrnuje normy, které:

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

b) poskytují přímou podporu, podrobné pokyny a/nebo interpretaci pro celkový proces ustavení, implementace, udržování a zlepšování ISMS;

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

d) se zabývají posuzováním shody ve vztahu k ISMS.

Termíny a definice uvedené v této mezinárodní normě:

– zahrnují běžně používané termíny a definice v řadě norem ISMS;

– nezahrnují všechny termíny a definice použité v rámci řady norem ISMS;

– neomezují řadu norem ISMS v definování nových termínů.

1 Předmět normy

Tato mezinárodní norma podává přehled systémů řízení bezpečnosti informací a termíny a definice běžně používané v řadě norem ISMS. Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací (například pro obchodní podniky, vládní úřady, neziskové organizace).