ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030

Březen 2018

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

ČSN ISO/IEC 27003

36 9790

Information Technology – Security techniques – Information security management systems – Guidance

Technologies de l'information – Techniques de sécurité – Systemes de management de la sécurité de l'information – Lignes directrices

Tato norma je českou verzí mezinárodní normy ISO/IEC 27003:2017. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27003:2017. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27003 (36 9790) z prosince 2011.

Národní předmluva

Změny proti předchozí normě

Rozsah a název druhého vydání ISO/IEC 27003 je v souladu s požadavky ISO/IEC 27001:2013. Struktura druhého vydání ISO/IEC 27003 je přizpůsobena struktuře normy ISO/IEC 27001:2013, aby se uživateli usnadnilo její použití společně s normou ISO/IEC 27001:2013.

Informace o citovaných dokumentech

ISO/IEC 27000:2016 zavedena v ČSN EN ISO/IEC 27000:2017 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2013 zavedena v ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Souvisící ČSN

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

ČSN EN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 27003:2011 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

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

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

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyny“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména normy řady ISO/IEC 27XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti s řadou norem ISO/IEC 27XXX nepoužívá.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

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.

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

ISO/IEC 27003
Druhé vydání
2017-03

ICS 35.100.70; 35.030

Obsah

Strana

1..... Předmět normy..... 8

2..... Citované dokumenty..... 8

3..... Termíny a definice..... 8

4..... Kontext organizace..... 8

4.1..... Pochopení organizace a jejího kontextu..... 8

4.2..... Pochopení potřeb a očekávání zainteresovaných stran..... 10

4.3..... Určení rozsahu systému řízení bezpečnosti informací..... 10

4.4..... Systém řízení bezpečnosti informací..... 12

5..... Vůdčí role..... 12

5.1..... Vůdčí role a závazek..... 12

5.2..... Politika.....

..... 13

5.3..... Organizační role, odpovědnosti
a pravomoci..... 14

6.....
Plánování.....
..... 15

6.1..... Činnosti pro řešení rizik
a příležitostí..... 15

6.1.1...
Obecně.....
..... 15

6.1.2... Posuzování rizik bezpečnosti
informací..... 17

6.1.3... Ošetření rizik bezpečnosti
informací..... 19

6.2..... Cíle bezpečnosti informací a plánování jejich
dosažení..... 22

7.....
Podpora.....
..... 24

7.1.....
Zdroje.....
..... 24

7.2.....
Kompetence.....
..... 24

7.3.....
Povědomí.....
..... 25

7.4.....
Komunikace.....
..... 26

7.5..... Dokumentované
informace.....
..... 27

7.5.1...
Obecně.....
..... 27

7.5.2… Vytváření
a aktualizace…… 28

7.5.3… Řízení dokumentovaných
informací…… 29

8……
Provozování……
…… 30

8.1…… Plánování a řízení
provozu……
….. 30

8.2…… Posuzování rizik bezpečnosti
informací…… 31

8.3…… Ošetření rizik bezpečnosti
informací…… 32

9…… Hodnocení
výkonnosti……
…… 32

9.1…… Monitorování, měření, analýza
a hodnocení…… 32

9.2..... Interní audit..... 33

9.3..... Přezkoumání vedením organizace..... 35

10..... Zlepšování..... 37

10.1.... Neshody a nápravná opatření..... 37

10.2.... Neustálé zlepšování..... 39

Příloha A (informativní) Rámec politik..... 40

Bibliografie..... 42

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2017, Published in Switzerland
Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.
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 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. 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 dobrovolné povahy norem, 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: www.iso.org/iso/foreword.html.

Tento dokument vypracovala ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Toto druhé vydání ISO/IEC 27003 zrušuje a nahrazuje první vydání (ISO/IEC 27003:2010) a je jeho revizí menšího rozsahu.

Hlavní změny oproti předchozímu vydání jsou následující:

- rozsah a název byly změněny tak, aby pokryly vysvětlení normy ISO/IEC 27001:2013 a zahrnuly pokyny k požadavkům této normy, namísto k předchozímu vydání (ISO/IEC 27001:2005);

- struktura je nyní přizpůsobena struktuře normy ISO/IEC 27001:2013, aby se uživateli usnadnilo její použití společně s normou ISO/IEC 27001:2013;

- předchozí vydání mělo projektový přístup se sledem činností. Toto vydání poskytuje pokyny k požadavkům bez ohledu na pořadí, ve kterém jsou implementovány.

Úvod

Tento dokument představuje pokyny k požadavkům na systém řízení bezpečnosti informací (ISMS), jak je specifikován v ISO/IEC 27001, a poskytuje doporučení („měl by“), možnosti („může“) a oprávnění („smí“) ve vztahu k nim. Účelem tohoto dokumentu není poskytnout obecné pokyny týkající se všech aspektů bezpečnosti informací.

Kapitoly 4 až 10 tohoto dokumentu odrážejí strukturu normy ISO/IEC 27001:2013.

Tento dokument nepřidává žádné nové požadavky na ISMS a s ním souvisící termíny a definice. Organizace by měly odkazovat na požadavky a definice podle ISO/IEC 27001 a ISO/IEC 27000. Organizace implementující ISMS nejsou povinny dodržovat pokyny uvedené v tomto dokumentu.

ISMS zdůrazňuje důležitost následujících fází:

- pochopení potřeb organizace a nutnosti ustanovení politiky bezpečnosti informací a cílů bezpečnosti informací;
- posouzení rizik organizace v oblasti bezpečnosti informací;
- implementace a provozování procesů, kontrol a dalších opatření pro ošetření rizik v oblasti bezpečnosti informací;
- monitorování a přezkoumávání výkonnosti a efektivnosti ISMS; a
- praktikovat neustálé zlepšování.

ISMS, podobně jako jakýkoliv jiný typ systému řízení, zahrnuje následující klíčové komponenty:

a) politiku;

b) osoby s definovanými odpovědnostmi;

c) procesy řízení týkající se:

1) ustanovení politiky;

2) poskytování povědomí a kompetencí;

3) plánování;

4) implementace;

5) provozování;

6) posuzování výkonu;

7) přezkoumání vedením; a

8) zlepšování; a

d) dokumentované informace.

ISMS má další klíčové komponenty, jako je:

e) posuzování rizik bezpečnosti informací; a

f) ošetření rizik bezpečnosti informací, včetně určení a implementace kontrolních opatření.

Tento dokument je obecný a má být použitelný pro všechny organizace bez ohledu na typ, velikost nebo povahu. Organizace by měla určit, která část těchto pokynů se na ni v souladu s jejím specifickým organizačním kontextem vztahuje (viz ISO/IEC 27001:2013, kapitola 4).

Některé pokyny mohou být například vhodnější pro velké organizace, ale u velmi malých organizací (například s méně než 10 osobami) mohou být některé pokyny nepodstatné nebo nevhodné.

Popisy kapitol 4 až 10 jsou strukturovány následovně:

- **Požadovaná činnost**: představuje klíčové činnosti požadované v odpovídajících článcích ISO/IEC 27001;

- **Vysvětlení**: vysvětluje, co implikují požadavky ISO/IEC 27001;

- **Pokyny**: poskytují podrobnější nebo podpůrné informace pro implementaci „požadované činnosti“ včetně příkladů implementace; a

- **Další informace**: poskytují další informace, které lze vzít v úvahu.

ISO/IEC 27003, ISO/IEC 27004 a ISO/IEC 27005 tvoří soubor dokumentů, které podporují ISO/IEC 27001:2013 a poskytují k ní pokyny. Mezi těmito dokumenty představuje ISO/IEC 27003 základní a komplexní dokument, který poskytuje pokyny pro všechny požadavky ISO/IEC 27001, ale neobsahuje podrobné popisy týkající se „monitorování, měření, analýzy a hodnocení“ a řízení rizik bezpečnosti informací. ISO/IEC 27004 a ISO/IEC 27005 se zaměřují na konkrétní obsah a poskytují podrobnější pokyny týkající se „monitorování, měření, analýzy a hodnocení“ a řízení rizik bezpečnosti informací.

V ISO/IEC 27001 je několik explicitních odkazů na dokumentované informace. Nicméně organizace může uchovávat dodatečně dokumentované informace, které určí za nezbytné pro efektivnost svého systému řízení jako součást své reakce na ISO/IEC 27001:2013, 7.5.1 b). V těchto případech se v tomto dokumentu používá fráze „Dokumentované informace o této činnosti a její výsledek je povinný pouze ve formě a rozsahu, který organizace určí za nezbytné pro efektivnost svého systému řízení (viz ISO/IEC 27001:2013, 7.5.1 b)).“

1 Předmět normy

Tento dokument poskytuje vysvětlení a pokyny k normě ISO/IEC 27001:2013.

Konec náhledu - text dále pokračuje v placené verzi ČSN.