ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Září 2014**

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

ČSN ISO/IEC 27001
36 9797

Information technology – Security techniques – Information security management systems – Requirements

Technologies de l,information – Techniques de sécurité – Systemes de management de la sécurité de l,information – Exigences

Tato norma je českou verzí mezinárodní normy ISO/IEC 27001:2013. 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 International Standard ISO/IEC 27001:2013. 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 27001 (36 9790) z října 2006.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání nahrazuje první vydání (ČSN ISO/IEC 27001:2006), které bylo technicky revidováno. Základní změnou je změna termínů a definic a jejich použití v normě.

Informace o citovaných dokumentech

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

Souvisící ČSN

ČSN ISO/IEC 27002:2014 (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 31000:2010 (01 0351) Management rizik – Principy a směrnice

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s. r. o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27001
Systémy řízení bezpečnosti informací – Požadavky Druhé vydání
2013-10-01

ICS 35.040

Obsah

Strana

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

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.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 27001 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27001:2005), které bylo revidováno.

0 Úvod

0.1 Obecně

Tato mezinárodní norma byla připravena, aby poskytla požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Přijetí systému řízení bezpečnosti informací je pro organizaci strategickým rozhodnutím. Ustavení a implementace systému řízení bezpečnosti informací 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 řízení bezpečnosti informací zachovává důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dává jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena.

Je důležité, že systém řízení bezpečnosti informací je součástí procesů a celkové struktury řízení organizace a je do nich integrován. Je také důležité, že bezpečnost informací je zvažována při návrhu procesů, informačních systémů a opatření. Očekává se, že implementace systému řízení bezpečnosti informací bude nastavena v souladu s potřebami organizace.

Tato mezinárodní norma může být použita interními a externími stranami k posouzení schopnosti organizace splnit její vlastní požadavky bezpečnosti informací.

Pořadí, ve kterém jsou uvedeny požadavky této mezinárodní normy, neodráží jejich důležitost nebo nenaznačuje pořadí, ve kterém by měly být implementovány. Položky seznamu jsou vyjmenovány pouze pro referenční účely.

ISO/IEC 27000 popisuje přehled a slovník systémů řízení bezpečnosti informací a odkazuje na řadu norem systému řízení bezpečnosti informací (včetně ISO/IEC 27003[2], ISO/IEC 27004[3] a ISO/IEC 27005[4]) s odpovídajícími termíny a definicemi.

0.2 Kompatibilita s jinými normami systémů řízení

Tato mezinárodní norma aplikuje strukturu vyšší úrovně, totožné názvy článků, totožný text, společné termíny a hlavní definice přesně vymezené v příloze SL v části 1 Směrnic ISO/IEC, Konsolidovaný ISO dodatek, a proto udržuje kompatibilitu s ostatními normami systémů řízení, které přijaly tuto přílohu SL.

Tento společný přístup definovaný v příloze SL bude užitečný pro ty organizace, které se rozhodnou provozovat jediný řídicí systém, který splňuje požadavky dvou a více norem systémů řízení.

1 Předmět normy

Tato mezinárodní norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v rámci kontextu organizace. Tato mezinárodní norma také zahrnuje požadavky na posuzování a ošetření rizik bezpečnosti informací, přizpůsobené potřebám organizace. Požadavky této mezinárodní normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků specifikovaných v kapitolách 4 až 10 je nepřijatelné, pokud chce organizace dosáhnout shody s touto normou.