ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Duben 2021**

Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Použití ISO/IEC 27001 v jednotlivých odvětvích – Požadavky	ČSN ISO/IEC 27009 36 9790

Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements

Sécurité de l,information, cybersécurité et protection des données personnelles – Application de l,ISO/IEC 27001
a un secteur spécifique – Exigences

Tato norma je českou verzí mezinárodní normy ISO/IEC 27009:2020. 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 27009:2020. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

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

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

Souvisící ČSN

ČSN EN ISO/IEC 27011 (36 9710) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro telekomunikační organizace založený na ISO/IEC 27002

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 EN 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/IEC 27019 (36 9719) Informační technologie – Bezpečnostní techniky – Opatření bezpečnosti
informací pro energetický průmysl

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).

Vysvětlivky k textu převzaté normy

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

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 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

Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – ISO/IEC 27009 Použití ISO/IEC 27001 v jednotlivých odvětvích – Požadavky Druhé vydání 2020-04

ICS 35.030

Obsah

Strana

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 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), viz www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí.*

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27009:2016), které bylo technicky zrevidováno.

Hlavní změny oproti předchozímu vydání jsou následující:

- předmět normy byl aktualizován, aby jasněji odrážel obsah tohoto dokumentu;
- dřívější příloha A byla rozdělena na přílohy A a B;
- byla vytvořena příloha C.

Jakákoliv zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směrovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

1 Předmět normy

Tento dokument specifikuje požadavky na vytváření norem specifických pro jednotlivá odvětví, které rozšiřují ISO/IEC 27001 a doplňují nebo pozměňují ISO/IEC 27002 tak, aby podporovaly konkrétní odvětví (obor, oblast použití nebo trh).

Tento dokument vysvětluje, jak:

- zahrnout požadavky navíc k požadavkům v ISO/IEC 27001,
- upřesnit nebo interpretovat kterýkoli z požadavků ISO/IEC 27001,
- zahrnout opatření navíc k opatřením uvedeným v ISO/IEC 27001:2013, příloha A a v ISO/IEC 27002,
- modifikovat kterékoli z opatření uvedené v ISO/IEC 27001:2013, příloha A a v ISO/IEC 27002,
- přidat pokyny nebo upravit pokyny uvedené v ISO/IEC 27002.

Tento dokument specifikuje, že doplňující nebo upřesněné požadavky nezneplatňují požadavky ISO/IEC 27001.

Tento dokument je použitelný pro ty, kdo se podílejí na vytváření norem specifických pro jednotlivá odvětví.