ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80 **Říjen 2010**

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

ČSN
EN ISO 27799
98 2021

idt ISO 27799:2008

Health informatics – Information security management in health using ISO/IEC 27002

Informatique de santé – Gestion de la sécurité de l,information relative a la santé en utilisant l,ISO/IEC 27002

Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei verwendung der ISO/IEC 27002

Tato norma je českou verzí evropské normy EN ISO 27799:2008. 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 27799:2008. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 27799 (98 2021) z ledna 2009.

Národní předmluva

Změny proti předchozím normám

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 27799:2008 do soustavy norem ČSN. Zatímco ČSN EN ISO 27799 z ledna 2009 převzala EN ISO 27799:2008:2008 schválením k přímému používání oznámením ve Věstníku ÚNMZ, jako ČSN, tato norma ji přejímá překladem.

Informace o citovaných normativních dokumentech

ISO/IEC 27002 zavedena v ČSN ISO/IEC 17799 (36 9790) – Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

Související ČSN

ČSN ISO/TR 18307:2003 (98 1018) Zdravotnická informatika – Interoperabilita a slučitelnost v normách pro předávání zpráv a komunikací – Klíčové charakteristiky

ČSN ISO/IEC 27001:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 15408-2:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ČSN ISO/IEC 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

Vysvětlivky k textu převzaté normy

Vzhledem k vývoji terminologie v oblasti IT, se slovo management překládá podle kontextu, ve kterém bylo použito. V tomto případě bylo slovo management v názvu této normy nahrazeno slovem řízení, což je v souladu s procesem vytváření názvů pro normy řady ISO/IEC 27000. U norem ČSN ISO/IEC 27001 a ČSN ISO/IEC 17799 (ISO/IEC 27002) bude úprava provedena při jejich revizi.

Tato norma je rozšířením zavedené normy ČSN ISO/IEC 27002 k zajištění důvěrnosti, integrity a dostupnosti osobních (zdravotnických) informací v oblasti poskytování zdravotní péče.

Termín**byznys (e-byznys)** je v prostředí tvorby norem a normalizačních dokumentů chápán jako série procesů, z nichž každý má zřejmý a srozumitelný účel; je realizovaná pomocí výměny informací, směrovaná ke vzájemně odsouhlasenému cíli, probíhá po určitý časový úsek a zahrnuje více než jednu stranu.

Vypracování normy

Zpracovatel: Berkely Cert s. r. o., IČ 28882458, Ing. Daniel Kardoš

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

EVROPSKÁ NORMA EN ISO 27799
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Červenec 2008

ICS 35.240.80

Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002 (ISO 27799:2008)

Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799:2008)

Informatique de santé – Gestion de la sécurité de l,information relative a la santé en utilisant l,ISO/IEC 27002 (ISO 27799:2008)

Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei verwendung der ISO/IEC27002 (ISO 27799:2008)

Tato evropská norma byla schválena CEN 2008-06-15.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CEN

Evropský výbor pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Řídicí centrum: rue de Stassart, 36 B-1050 Brusel

Ref. č. EN ISO 27799:2008: E

Předmluva

Tento dokument (EN ISO 27799:2008) byl připraven technickou komisí ISO/TC 215 „Zdravotnická informatika“ ve spolupráci s technickou komisí CEN/TC 251 „Zdravotnická informatika“ jejímž sekretariátem je NEN.

Této evropské normě je nutno nejpozději do ledna 2008 dát 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 ledna 2008.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN (a/nebo CENELEC) není odpovědný za identifikování jakýchkoli nebo všech patentových práv.

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

Oznámení o schválení

Text ISO 21549-6:2008 byl schválen CEN jako EN ISO 21549-6:2008 bez jakýchkoliv modifikací.

MEZINÁRODNÍ NORMA

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

První vydání
2008-07

ICS 35.240.80

ISO copyright office

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

Obsah

Strana

Bibliografie 55

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (členů ISO). Na mezinárodních normách obvykle pracují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být zastoupen v této komisi. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO navázalo pracovní styk. ISO úzce spolupracuje s Mezinárodní komisí pro elektrotechniku (IEC) ve všech záležitostech elektrotechnické normalizace.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem technických komisí je vypracování mezinárodních norem. Návrhy mezinárodních norem, přijaté technickými komisemi, se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Je nutné upozornit na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových oprávnění. ISO neodpovídá za případ identifikace některých nebo všech takových patentových oprávnění.

ISO 27799 byla připravena Technickou komisí ISO/TC 215, *Zdravotnická informatika*.

Úvod

Tato mezinárodní norma poskytuje pokyny zdravotnickým a jiným organizacím, jak nejlépe zajistit důvěrnost, integritu a dostupnost osobních zdravotních informací zavedením ISO/IEC 27002[1)]. Tato norma se zaměřuje na management bezpečnosti informací v rezortu zdravotnictví a v jeho specifických provozních podmínkách. Zatímco ochrana a bezpečnost osobních informací je důležitá pro všechny jednotlivce, společnosti, instituce a vlády, v sektoru zdravotnictví musí být splněny zvláštní požadavky, aby tak byla zajištěna důvěrnost, integrita, auditovatelnost a dostupnost osobních zdravotních informací. Zdravotnické informace jsou považovány za nejdůvěrnější ze všech druhů osobních informací. Ochrana této důvěrnosti je nezbytná, pokud má být zajištěno soukromí subjektů zdravotní péče. Integrita zdravotnických informací musí být chráněna, aby tak bylo zajištěno bezpečí pacientů. Důležitou součástí této ochrany je i zajištění auditovatelnosti celého životního cyklu informací. Dostupnost zdravotnických informací je také rozhodující z hlediska efektivity výkonu zdravotní péče. Systémy zdravotnické informatiky musí splňovat zvláštní požadavky, aby byly akceschopné při přírodních katastrofách, systémových selháních a při útocích typu odmítnutí služby. Ochrana důvěrnosti, integrity a dostupnosti zdravotnických informací tudíž vyžaduje odbornou způsobilost v oblasti rezortu zdravotnictví.

Potřeba efektivního managementu bezpečnosti IT ve zdravotnictví naléhavě stoupá s rostoucím počtem bezdrátových a internetových technologií v poskytování zdravotní péče. Pokud nejsou správně zavedeny, zvyšují tyto technologie rizika důvěrnosti, integrity a dostupnosti zdravotnických informací. Ve všech zdravotnických organizacích jsou nezbytné přísné kontroly přímo v místě s cílem chránit jim svěřené zdravotnické informace bez ohledu na velikost, umístění a formu poskytování služeb. Existuje mnoho odborných zdravotnických pracovníků, kteří fungují samostatně nebo v malých klinikách a kterým chybí specializované IT zdroje na řízení bezpečnosti informací. Zdravotnické organizace proto musí mít jasné, stručné a zdravotně-specifické pokyny týkající se výběru a provádění těchto kontrol. Tento návod musí být přizpůsobitelný široké škále poskytovatelů služeb ve zdravotnictví, různé velikosti, umístění či formy. Konečně v souvislosti s elektronickou výměnou osobních zdravotních údajů mezi odbornými zdravotnickými pracovníky je zde jasný přínos v přijetí

společných doporučení pro řízení bezpečnosti informací v oblasti zdravotní péče.

ISO/IEC 27002 je již široce používána pro zdravotnickou informatiku managementu bezpečnosti IT prostřednictvím působení národních či regionálních směrnic v Austrálii, Kanadě, Francii, Nizozemí, Novém Zélandu, Jižní Africe a Velké Británii. Zájem roste i v jiných zemích. Tato mezinárodní norma (ISO 27799) staví na zkušenostech těchto států a jejich úsilí při řešení bezpečnosti osobních zdravotních informací a je určena jako doprovodný dokument k ISO/IEC 27002. Není určena k nahrazení ISO/IEC 27002 nebo ISO/IEC 27001. Spíše se jedná o doplnění těchto obecnějších norem.

Tato mezinárodní norma aplikuje ISO/IEC 27002 do oblasti zdravotní péče způsobem, který pečlivě zvažuje vhodné uplatnění bezpečnostních kontrol za účelem ochrany osobních zdravotních informací. V některých případech vedly tyto úvahy jeho autory k závěru, že použití určitých kontrolních cílů ISO/IEC 27002 je nezbytné, pokud mají být osobní zdravotní informace odpovídajícím způsobem chráněny. Tato mezinárodní norma tudíž klade omezení v aplikaci některých bezpečnostních kontrol definovaných v ISO/IEC 27002. To následně vedlo k několika normativním prohlášením o povinnosti používání dané bezpečnostní kontroly v kapitole 7. Například 7.2.1 uvádí, že:

> *Organizace, které zpracovávají zdravotnické informace, včetně osobních údajů,* ***musí*** *mít politiku bezpečnosti informací, která je schválena vedením, publikována a sdělena všem zaměstnancům a příslušným vnějším stranám.*

V oblasti zdravotnictví je možné, aby organizace (řekněme nemocnice), byla certifikována ISO/IEC 27001 bez předchozího schválení, nebo dokonce i bez přijetí této mezinárodní normy. Je třeba doufat, že se mezi zdravotnickými organizacemi rozšíří jak snaha o zlepšení bezpečnosti osobních zdravotních informací, tak i přísnější kritéria pro poskytování zdravotní péče.

Všechny cíle bezpečnostní kontroly popsané v ISO/IEC 27002 jsou důležité pro zdravotnickou informatiku, ale některé kontroly vyžadují další vysvětlení, aby mohly být použity co nejlépe k ochraně důvěrnosti, integrity a dostupnosti zdravotnických informací. Existují i další specifické požadavky. Tato mezinárodní norma poskytuje další pokyny, které jsou snadno pochopitelné a přijatelné pro osoby odpovědné za bezpečnost zdravotnických informací.

Autoři normy nemají v úmyslu psát učebnici počítačového zabezpečení, ani přepisovat to, co už bylo uvedeno v ISO/IEC 27002 a ISO/IEC 27001. Existuje mnoho bezpečnostních požadavků, které jsou společné pro všechny počítačové systémy, ať již jsou používány v oblasti finančních služeb, výroby, průmyslu nebo v jakémkoliv jiném organizovaném úsilí. Zde je zaměřena intenzivní pozornost na bezpečnostní požadavky, vyžadované specifickými výzvami při předávání elektronických zdravotnických informací, které podporují poskytnutí péče.

Kdo by měl číst tuto mezinárodní normu?

Tato mezinárodní norma je určena osobám odpovědným za kontrolování bezpečnosti zdravotnických informací, zdravotnickým organizacím a dalším správcům zdravotnických informací, hledajícím radu k tomuto tématu, spolu s jejich bezpečnostními poradci, konzultanty, auditory, prodejci a třetími stranami poskytujícími služby.

Výhody používání této mezinárodní normy

ISO/IEC 27002 je široká a komplexní norma a informace v ní obsažené nejsou specificky uzpůsobené pro účely zdravotnictví. Tato mezinárodní norma umožňuje zavedení ISO/IEC 27002 do prostředí zdravotnictví konzistentním způsobem a se zvláštním zřetelem na specifika této oblasti. Její implementace pomáhá zdravotnickým organizacím zajistit dodržování důvěrnosti a integrity dat při

jejich péči, zachování dostupnosti kritických zdravotnických informačních systémů a prosazovat odpovědnost za zdravotnické informace.

Přijetí této směrnice zdravotnickými organizacemi jak uvnitř, tak i vně jurisdikce přispěje součinnosti a umožní bezpečné přijetí nových spolupracujících technologií v oblasti poskytování zdravotní péče. Bezpečné a soukromí ochraňující sdílení informací může výrazně zlepšit lékařské výsledky.

V důsledku zavedení této směrnice mohou zdravotnické organizace očekávat snížení počtu bezpečnostních incidentů a jejich závažnosti, což umožní přesunout zdroje do produktivních činností. Bezpečnost IT pak umožní rozmístění zdravotnických prostředků rentabilním a efektivním způsobem. Průzkum provedený uznávaným Fórem bezpečnosti informací a tržními analytiky ukázal, že dobré a všestranné zabezpečení může mít více než dvouprocentní pozitivní dopad na výsledky hospodaření organizace.

Důsledný přístup k bezpečnosti IT, který je srozumitelný pro všechny zúčastněné subjekty, povede ke zlepšení pracovní morálky a zvýšení důvěry veřejnosti v systémy, které spravují osobní zdravotní informace.

Jak používat tuto mezinárodní normu

Čtenářům, kteří ještě nejsou seznámeni s ISO/IEC 27002 je doporučeno, aby si nejprve přečetli její úvodní část. Implementátoři této normy (ISO/IEC 27799) musí být důkladně seznámeni s obsahem ISO/IEC 27002, protože dále v textu jsou často uvedeny odkazy na příslušné oddíly normy. Současný dokument nemůže být plně pochopen bez přístupu k plnému znění ISO/IEC 27002.

Čtenáři, kteří ještě nejsou dobře seznámeni s bezpečností zdravotnických informací, jejími cíli, úkoly a širším kontextem, najdou tyto informace ve stručném úvodu, který se nachází v kapitole 5.

Čtenáři, hledající radu, jak implementovat ISO/IEC 27002 do zdravotnického prostředí, najdou praktický akční plán v kapitole 6. V této kapitole nejsou uvedeny žádné závazné požadavky. Jsou zde obecné rady a pokyny, jak nejlépe provést implementaci normy 27002 ve zdravotnictví. Kapitola je uspořádána v rámci cyklu aktivit „plánuj-dělej-kontroluj-jednej“ (plan/do/check/act), které jsou popsány v ISO/IEC 27001. Jejich dodržování povede k plné implementaci systému řízení bezpečnosti informací.

V kapitole 7 najdou čtenáři konkrétní rady k jedenácti kapitolám a 39 hlavním bezpečnostním kategoriím, které jsou popsané v ISO/IEC 27002. Tato část je provede přes všech jedenáct kapitol bezpečnostní kontroly ISO/IEC 27002. Jsou zde uvedeny minimální požadavky a u některých případů i normativní směrnice pro správné zavedení určitých bezpečnostních kontrol ISO/IEC 27002 pro ochranu zdravotnických informací.

Tuto mezinárodní normu uzavírají tři informativní přílohy. Příloha A popisuje obecné hrozby pro zdravotnické informace. Příloha B stručně popisuje úkoly a související dokumenty systému řízení bezpečnosti zdravotnických informací. Příloha C popisuje výhody podpůrných nástrojů jako pomoc při implementaci. Bibliografie shrnuje související normy v oblasti bezpečnosti zdravotnických informací.

1 Předmět normy

1.1 Všeobecně

Tato mezinárodní norma definuje obecné zásady pro podporu interpretace a implementace zdravotnické informatiky ISO/IEC 27002 a je doprovodem této normy[).

Tato norma specifikuje soubor podrobných kontrol pro řízení bezpečnosti zdravotnických informací a poskytuje směrnice pro prověřené postupy v oblasti bezpečnosti zdravotnických informací. Zavedením této normy budou zdravotnické organizace a ostatní správci zdravotnických informací schopni zajistit nezbytnou minimální úroveň zabezpečení, která odpovídá poměrům v organizaci a zachová důvěrnost, integritu a dostupnost osobních zdravotních informací.

Tato norma se vztahuje na zdravotnické informace ve všech aspektech, bez ohledu na jejich formu (slovní a číselnou, zvukové nahrávky, kresby, video a lékařské snímky), na prostředky k jejich ukládání (tisk, zápis na papíře nebo elektronické uložení) a na prostředky využívané k jejich přenosu (ručně, faxem, přes počítačové sítě či poštou), protože tyto údaje musí být vždy náležitě chráněny.

Normy ISO/IEC 27002 a ISO/IEC 27799 společně určují, *jaké* jsou požadavky na bezpečnost informací ve zdravotnictví, ale již nedefinují, *jak* by měly být tyto požadavky splněny. To znamená, že tato norma je v co největším rozsahu technologicky neutrální. Neutralita ve vztahu k zavádění technologií je důležitým rysem. Bezpečnostní technologie stále prochází rychlým vývojem a jeho tempo se v současné době měří spíše v měsících, než v letech. Oproti tomu normy, přestože jsou předmětem periodických revizí, by měly celkově zůstat v platnosti celé roky. Důležité také je, že tato technologická neutralita umožňuje prodejcům a poskytovatelům služeb navrhovat nové a rozvíjející se služby, které budou splňovat nezbytné požadavky popsané v této normě.

Jak již bylo uvedeno v úvodu, dobrá znalost ISO/IEC 27002 je k pochopení této normy nezbytná.

1.2 Výjimky

Následující oblasti bezpečnosti informací jsou mimo rozsah této normy:

a. metodika a statistické testy pro efektivní anonymizaci osobních zdravotních informací;
b. metodika pro pseudonymizaci osobních zdravotních informací (viz ISO/TS 25237 – příklad ISO Technické specifikace, která konkrétně pojednává o tomto tématu);
c. kvalita služeb a metody pro měření dostupnosti sítí pro zdravotní informatiku;
d. kvalita dat (na rozdíl od integrity dat).