

STN	Informačné technológie Bezpečnostné metódy Kódex postupov pre opatrenia informačnej bezpečnosti založený na norme ISO/IEC 27002 pre cloudové služby (ISO/IEC 27017: 2015)	STN EN ISO/IEC 27017 97 4112
------------	--	--

Information technology

Security techniques

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information

Techniques de sécurité

Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Informationstechnik

Sicherheitsverfahren

Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27017: 2021.

Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.

STN EN ISO/IEC 27017 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27017: 2021.

It was translated by Slovak Office of Standards, Metrology and Testing.

STN EN ISO/IEC 27017 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 27017 z augusta 2021 v celom rozsahu.

140294

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2025

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2015 ISO/IEC, ref. č. ISO/IEC 27017: 2015 E.

ISO/IEC 27017 vypracovala spoločná technická komisia ISO/IEC JTC 1 *Informačné technológie*, subkomisia SC 27 *Bezpečnostné metódy IT*, v spolupráci s ITU-T. Identický text je uverejnený ako ITU-T. X.1631 (07/2015).

Text kapitol 5 až 18 je zosúladený s normou ISO/IEC 27002: 2013, ktorá bola v čase vydania EN ISO/IEC 27017: 2021 platná.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 17788 prijatá ako STN ISO/IEC 17788

POZNÁMKA 3. – ISO/IEC 17788 bola zrušená a nahradená ISO/IEC 22123-1 a ISO/IEC 22123-2 prijaté ako STN ISO/IEC 22123-1 *Informačné technológie. Cloud computing. Časť 1: Slovník* (97 4176) a STN ISO/IEC 22123-2 *Informačné technológie. Cloud computing. Časť 2: Koncepty* (97 4176).

ISO/IEC 17789 dosiaľ neprijatá

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 *Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník* (ISO/IEC 27000) (97 4170)

ISO/IEC 27002: 2013 prijatá ako STN EN ISO/IEC 27002: 2019

POZNÁMKA 4. – ISO/IEC 27002: 2013 bola zrušená a nahradená ISO/IEC 27002: 2022 prijatá ako STN ISO/IEC 27002: 2023 *Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti* (ISO/IEC 27002: 2022) (97 4172).

Vypracovanie

Spracovateľ: SynCo, s.r.o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 *Informačné technológie*

**Informačné technológie
Bezpečnostné metódy
Kódex postupov pre opatrenia informačnej bezpečnosti
založený na norme ISO/IEC 27002 pre cloudové služby
(ISO/IEC 27017: 2015)**

Information technology
Security techniques

Code of practice for information security controls based on ISO/IEC 27002 for cloud services
(ISO/IEC 27017: 2015)

Technologies de l'information
Techniques de sécurité
Code de pratique pour les contrôles de sécurité
de l'information fondés sur l'ISO/IEC 27002
pour les services du nuage
(ISO/IEC 27017: 2015)

Informationstechnik
Sicherheitsverfahren
Anwendungsleitfaden für Informations-
sicherheitsmaßnahmen basierend
auf ISO/IEC 27002 für Cloud Dienste
(ISO/IEC 27017: 2015)

Túto európsku normu schválil CEN 20. decembra 2020.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN a CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Maltu, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Obsah

strana

Európsky predhovor	6
Úvod	11
1 Predmet	12
2 Normatívne odkazy	12
2.1 Identické odporúčania Medzinárodné normy	12
2.2 Ďalšie odkazy	12
3 Definície a skratky	12
3.1 Termíny definované inde	12
3.2 Skratky	13
4 Koncepty špecifické pre odvetvie cloudových služieb	13
4.1 Prehľad	13
4.2 Vzťahy s dodávateľmi v cloudových službách	14
4.3 Vzťahy medzi zákazníkmi cloudových služieb a poskytovateľmi cloudových služieb	14
4.4 Riadenie rizík informačnej bezpečnosti v cloudových službách	15
4.5 Štruktúra tejto normy	15
5 Politika informačnej bezpečnosti	16
5.1 Usmernenie pre informačnú bezpečnosť	16
6 Organizácia informačnej bezpečnosti	17
6.1 Vnútoraná organizácia	17
6.2 Mobilné zariadenia a práca na diaľku	18
7 Personálna bezpečnosť	19
7.1 Pred nástupom do zamestnania	18
7.2 Počas zamestnania	19
7.3 Ukončenie a zmena zamestnania	20
8 Riadenie aktív	20
8.1 Zodpovednosť za aktíva	20
8.2 Klasifikácia informácií	21
8.3 Zaobchádzanie s médiami	21
9 Riadenie prístupov	22
9.1 Požiadavky na riadenie prístupu	22
9.2 Riadenie používateľských prístupov	22
9.3 Zodpovednosť používateľov	24
9.4 Riadenie systémových a aplikačných prístupov	24

10	Kryptografia.....	25
10.1	Kryptografické opatrenia.....	25
11	Fyzická bezpečnosť a bezpečnosť prostredia	26
11.1	Zabezpečené oblasti	26
11.2	Bezpečnosť zariadení	27
12	Bezpečnosť prevádzky	28
12.1	Prevádzkové postupy a zodpovednosť	28
12.2	Ochrana pred škodlivým softvérom	30
12.3	Zálohovanie.....	30
12.4	Zaznamenávanie dát a monitorovanie	31
12.5	Riadenie prevádzkového softvéru.....	33
12.6	Riadenie technickej zraniteľnosti.....	33
12.7	Audit informačných systémov.....	33
13	Komunikačná bezpečnosť.....	33
13.1	Riadenie bezpečnosti v sieťach.....	33
13.2	Prenos informácií	34
14	Akvízia, vývoj a údržba informačných systémov	35
14.1	Bezpečnostné požiadavky na informačné systémy	35
14.2	Bezpečnosť pri vývoji a pri podporných procesoch	35
14.3	Testovacie údaje.....	36
15	Riadenie vzťahov s dodávateľmi.....	37
15.1	Informačná bezpečnosť vo vzťahoch s dodávateľmi.....	37
15.2	Riadenie dodávateľských služieb	38
16	Riadenie incidentov informačnej bezpečnosti	38
16.1	Riadenie incidentov informačnej bezpečnosti a zlepšovania	38
17	Aspekty informačnej bezpečnosti v riadení kontinuity.....	40
17.1	Kontinuita informačnej bezpečnosti	40
17.2	Redundancia	41
18	Súlad.....	41
18.1	Súlad s právnymi a zmluvnými požiadavkami	41
18.2	Preskúmanie informačnej bezpečnosti	43
Príloha A – Rozšírený súbor opatrení cloudových služieb.....		44
Príloha B – Odkazy na riziká informačnej bezpečnosti súvisiace s cloud computingom		49
Literatúra.....		51

Európsky predhovor

Text ISO/IEC 27017: 2015 vypracovala technická komisia ISO/IEC JTC 1 Informačné technológie, medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27017: 2021 technickou komisiou CEN/CLC/JTC 13 Kybernetická bezpečnosť a ochrana údajov, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskôr do júla 2021 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do júla 2021.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN nezodpovedá za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédsko, Talianska a Turecko.

Oznámenie o schválení

Text medzinárodnej normy ISO/IEC 27017: 2015 schválil CEN ako EN ISO/IEC 27017: 2021 bez akýchkoľvek modifikácií.

ITU-T

SEKTOR NORMALIZÁCIE PRE TELEKOMUNIKÁCIE
MEDZINÁRODNEJ TELEKOMUNIKAČNEJ ÚNIE

X.1631

(07/2015)

SÉRIA X: DÁTOVÉ SIETE, OTVORENÉ SYSTÉMOVÉ KOMUNIKÁCIE A BEZPEČNOSŤ

Zabezpečenie cloud computingu –
Návrh zabezpečenia cloud computingu

Informačné technológie

Bezpečnostné metódy

**Kódex postupov pre opatrenia informačnej bezpečnosti
založený na norme ISO/IEC 27002 pre cloudové služby**

Odporúčanie ITU-T X.1631

ODPORÚČANIA ITU-T SÉRIA X

DÁTOVÉ SIETE, OTVORENÉ SYSTÉMOVÉ KOMUNIKÁCIE A BEZPEČNOSŤ

VEREJNÉ DÁTOVÉ SIETE	X.1-X.199
PREPOJENIE OTVORENÝCH SYSTÉMOV	X.200-X.299
PREPOJENIE MEDZI SIEŤAMI	X.300-X.399
SYSTÉMY SPRACOVANIA SPRÁV	X.400-X.499
ADRESÁRE	X.500-X.599
SIEŤOVÉ A SYSTÉMOVÉ ASPEKTY OSI	X.600-X.699
RIADENIE OSI	X.700-X.799
BEZPEČNOSŤ	X.800-X.849
APLIKÁCIE OSI	X.850-X.899
OTVORENÉ DISTRIBUOVANÉ SPRACOVANIE	X.900-X.999
SIEŤOVÁ A INFORMAČNÁ BEZPEČNOSŤ	
Všeobecné bezpečnostné aspekty	X.1000-X.1029
Zabezpečenie siete	X.1030-X.1049
Riadenie bezpečnosti	X.1050-X.1069
Telebiometria	X.1080-X.1099
BEZPEČNÉ APLIKÁCIE A SLUŽBY	
Zabezpečenie viacsmerového vysielania	X.1100-X.1109
Zabezpečenie domácej siete	X.1110-X.1119
Mobilné zabezpečenie	X.1120-X.1139
Webové zabezpečenie	X.1140-X.1149
Bezpečnostné protokoly	X.1150-X.1159
Zabezpečenie typu peer-to-peer	X.1160-X.1169
Bezpečnosť sieťového ID	X.1170-X.1179
Zabezpečenie IPTV	X.1180-X.1199
BEZPEČNOSŤ KYBERNETICKÉHO PRIESTORU	
Kybernetická bezpečnosť	X.1200-X.1229
Boj proti spamu	X.1230-X.1249
Riadenie identít	X.1250-X.1279
BEZPEČNÉ APLIKÁCIE A SLUŽBY	
Núdzová komunikácia	X.1300-X.1309
Zabezpečenie všadeprítomnej siete senzorov	X.1310-X.1339
Odporúčania týkajúce sa PKI	X.1340-X.1349
VÝMENA INFORMÁCIÍ O KYBERNETICKEJ BEZPEČNOSTI	
Prehľad kybernetickej bezpečnosti	X.1500-X.1519
Výmena zraniteľnosti/stavu	X.1520-X.1539
Výmena udalostí/incidentov/heuristik	X.1540-X.1549
Výmena politík	X.1550-X.1559
Heuristika a žiadosť o informácie	X.1560-X.1569
Identifikácia a objavenie	X.1570-X.1579
Zaručená výmena	X.1580-X.1589
BEZPEČNOSŤ CLOUD COMPUTINGU	
Prehľad zabezpečenia cloud computingu	X.1600-X.1601
Návrh zabezpečenia cloud computingu	X.1602-X.1639
Najlepšie postupy a návody na bezpečnosť cloud computingu	X.1640-X.1659
Implementácia zabezpečenia cloud computingu	X.1660-X.1679
Ostatné zabezpečenie cloud computingu	X.1680-X.1699

Ďalšie podrobnosti nájdete v zozname odporúčaní ITU-T.

MEDZINÁRODNÁ NORMA ISO/IEC 27017**ODPORÚČANIE ITU-T X.1631**

Informačné technológie
Bezpečnostné metódy
Kódex postupov pre opatrenia informačnej bezpečnosti
založený na norme ISO/IEC 27002 pre cloudové služby

Zhrnutie

Odporúčanie ITU-T X.1631 | ISO/IEC 27017 poskytuje návody na opatrenia informačnej bezpečnosti uplatniteľné na poskytovanie a používanie cloudových služieb tým, že poskytuje:

- ďalšie návody na implementáciu príslušných opatrení špecifikovaných v ISO/IEC 27002;
- ďalšie opatrenia s návodmi na implementáciu, ktoré sa konkrétne týkajú cloudových služieb.

Toto Odporúčanie | Medzinárodná norma poskytuje opatrenia a návod na implementáciu pre poskytovateľov aj zákazníkov cloudových služieb.

História

Edícia	Odporúčanie	Schválenie	Študijná skupina	Jedinečné ID ^{*)}
1.0	ITU-T X.1631	2015-07-14	17	11.1002/1000/11830-en

^{*)} Ak chcete získať prístup k odporúčaniu, zadajte do adresného poľa webového prehliadača adresu URL <http://handle.itu.int/>, za ktorou nasleduje jedinečné ID odporúčania. Napríklad <http://handle.itu.int/11.1002/1000/11830-en>.

Predhovor

Medzinárodná telekomunikačná únia (ITU) je špecializovanou agentúrou OSN v oblasti telekomunikácií, informačných a komunikačných technológií (IKT). Sektor ITU pre normalizáciu telekomunikácií (ITU-T) je stálym orgánom ITU. ITU-T je zodpovedná za skúmanie technických, prevádzkových a tarifných otázok a vydávanie odporúčaní k nim s cieľom normalizovať telekomunikácie na celosvetovej úrovni.

Svetové zhromaždenie pre štandardizáciu telekomunikácií (WTSA), ktoré sa schádza každé štyri roky, stanovuje témy na štúdium študijnými skupinami ITU-T, ktoré následne vypracúvajú odporúčania k týmto témam.

Na schvaľovanie odporúčaní ITU-T sa vzťahuje postup stanovený v rezolúcii 1 WTSA.

V niektorých oblastiach informačných technológií, ktoré patria do pôsobnosti ITU-T, sa potrebné normy pripravujú v spolupráci s ISO a IEC.

POZNÁMKA

V tomto odporúčaní sa výraz „správa“ používa z dôvodu stručnosti na označenie telekomunikačnej správy aj uznanej prevádzkovej agentúry.

Dodržiavanie tohto odporúčania je dobrovoľné. Odporúčanie však môže obsahovať určité povinné ustanovenia (napr. na zabezpečenie interoperability alebo použiteľnosti) a súlad s odporúčaním sa dosiahne, ak sú splnené všetky tieto povinné ustanovenia. Na vyjadrenie požiadaviek sa používajú slová „by mal“ alebo iný povinný jazyk, ako napríklad „musí“, a ich negatívne ekvivalenty. Použitie takýchto slov nenaznačuje, že súlad s odporúčaním sa vyžaduje od ktorejkoľvek strany.

PRÁVA DUŠEVNÉHO VLASTNÍCTVA

ITU upozorňuje na možnosť, že prax alebo vykonávanie tohto odporúčania môže zahŕňať používanie nárokovanej práva duševného vlastníctva. ITU nezaujíma žiadne stanovisko k dôkazom, platnosti alebo uplatniteľnosti nárokováných práv duševného vlastníctva, či už ich uplatňujú členovia ITU alebo iné osoby mimo procesu tvorby odporúčania.

Ku dňu schválenia tohto odporúčania ITU nedostala oznámenie o duševnom vlastníctve chránenom patentmi, ktoré môže byť potrebné na implementáciu tohto odporúčania. Upozorňujeme však vykonávateľov, že toto nemusí predstavovať najnovšie informácie, a preto sa im dôrazne odporúča, aby si pozreli patentovú databázu TSB na adrese <http://www.itu.int/ITU-T/ipr/>.

© ITU 2015

Všetky práva vyhradené. Žiadna časť tejto publikácie sa nesmie reprodukovat' akýmkoľvek spôsobom bez predchádzajúceho písomného súhlasu ITU.

Úvod

Návody obsiahnuté v tomto Odporúčaní | Medzinárodnej norme je doplnkom a rozšírením návodov uvedených v norme ISO/IEC 27002.

Toto Odporúčanie | Medzinárodná norma poskytuje najmä návody na podporu implementácie opatrení informačnej bezpečnosti pre zákazníkov cloudových služieb a poskytovateľov cloudových služieb. Niektoré návody sú určené pre zákazníkov cloudových služieb, ktorí zavádzajú opatrenia, a iné sú určené pre poskytovateľov cloudových služieb na podporu zavádzania týchto opatrení. Výber vhodných opatrení informačnej bezpečnosti a uplatnenie poskytnutých usmernení na implementáciu bude závisieť od posúdenia rizík a akýchkoľvek právnych, zmluvných, regulačných alebo iných špecifických požiadaviek na informačnú bezpečnosť v cloudovom sektore.

1 Predmet

Toto Odporúčanie | Medzinárodná norma poskytuje návody na opatrenia informačnej bezpečnosti, ktoré sa vzťahujú na poskytovanie a používanie cloudových služieb tým, že poskytuje:

- ďalšie návody na implementáciu príslušných opatrení špecifikovaných v ISO/IEC 27002;
- ďalšie opatrenia s návodmi k implementácii, ktoré sa konkrétne týkajú cloudových služieb.

Toto Odporúčanie | Medzinárodná norma poskytuje opatrenia a návod na implementáciu pre poskytovateľov aj zákazníkov cloudových služieb.

2 Normatívne odkazy

Nasledujúce odporúčania a medzinárodné normy obsahujú ustanovenia, ktoré prostredníctvom odkazu v tomto texte predstavujú ustanovenia tohto Odporúčania | Medzinárodnej normy. V čase uverejnenia boli platné uvedené vydania. Všetky Odporúčania a Normy podliehajú revízii a stranám dohôd založených na tomto Odporúčaní | Medzinárodnej norme sa odporúča preskúmať možnosť uplatnenia najnovšieho vydania nižšie uvedených Odporúčaní a Noriem. Členovia IEC a ISO vedú registre aktuálne platných medzinárodných noriem. Úrad pre normalizáciu telekomunikácií ITU vedie zoznam aktuálne platných odporúčaní ITU-T.

2.1 Identické Odporúčania | Medzinárodné normy

- Odporúčanie ITU-T Y.3500 (v platnosti) | ISO/IEC 17788: (v platnosti) *Information technology – Cloud computing – Overview and vocabulary*. [Informačné technológie. Informatický cloud. Prehľad a slovník.]
- Odporúčanie ITU-T Y.3502 (v platnosti) | ISO/IEC 17789: (v platnosti) *Information technology – Cloud computing – Reference architecture*. [Informačné technológie. Informatický cloud. Referenčná architektúra.]

2.2 Ďalšie odkazy

- ISO/IEC 27000: (v platnosti) *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.]
- ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security controls*. [Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.]

koniec náhľadu – text ďalej pokračuje v platenej verzii STN