ICS 03.120.20; 35.030 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA December 2025

STN P	**Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti Časť 2: Systémy riadenia bezpečnosti osobných údajov (ISO/IEC TS 27006-2: 2021)**	**STN P CEN ISO/IEC/TS 27006-2** 97 4185

Requirements for bodies providing audit and certification of information security management systems
Part 2: Privacy information management systems

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité
Partie 2: Systèmes de management des informations de sécurité

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren
Teil 2: Datenschutz-Managementsysteme

Táto predbežná slovenská technická norma je slovenskou verziou CEN ISO/IEC/TS 27006-2: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN P CEN ISO/IEC/TS 27006-2 má rovnaké postavenie ako majú oficiálne verzie.

This prestandard is the Slovak version of CEN ISO/IEC/TS 27006-2: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN P CEN ISO/IEC/TS 27006-2 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto predbežná slovenská technická norma nahrádza anglickú verziu STN P CEN ISO/IEC/TS 27006-2 z februára 2023 v celom rozsahu.

141415

Národný predhovor

Obrázky a matematické výrazy v tejto STN P sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2021 ISO/IEC, ref. č. ISO/IEC TS 27006-2: 2021 E.

Norma obsahuje tri národné poznámky.

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 17021-1 prijatá ako STN EN ISO/IEC 17021-1 Posudzovanie zhody. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky (ISO/IEC 17021-1) (01 5257)

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 27001 prijatá ako STN EN ISO/IEC 27001 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001) (97 4171)

ISO/IEC 27006: 2015 prijatá ako STN EN ISO/IEC 27006: 2021

POZNÁMKA 3. – ISO/IEC 27006: 2015 bola zrušená a nahradená ISO/IEC 27006: 2024 prijatá ako STN EN ISO/IEC 27006-1: 2024 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti. Časť 1: Všeobecne (ISO/IEC 27006-1: 2024) (97 4185)

ISO/IEC 27701 prijatá ako STN EN ISO/IEC 27701 Bezpečnostné metódy. Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov. Požiadavky a usmernenia (ISO/IEC 27701) (97 4123)

ISO/IEC 29100 prijatá ako STN EN ISO/IEC 29100 Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov (ISO/IEC 29100) (36 9758)

Vypracovanie

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

Technická komisia: TK 37 Informačné technológie

TECHNICKÁ ŠPECIFIKÁCIA
TECHNICAL SPECIFIKATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN ISO/IEC/TS 27006-2

November 2022

ICS 03.120.20; 35.030

Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti Časť 2: Systémy riadenia bezpečnosti osobných údajov (ISO/IEC TS 27006-2: 2021)

Requirements for bodies providing audit and certification
of information security management systems
Part 2: Privacy information management systems
(ISO/IEC TS 27006-2: 2021)

Exigences pour les organismes procédant
à l'audit et à la certification des systèmes
de management des informations de sécurité
Partie 2: Systèmes de management
des informations de sécurité
(ISO/IEC TS 27006-2: 2021)

Anforderungen an Stellen, die Informationssicherheits-
Managementsysteme auditieren und zertifizieren
Teil 2: Datenschutz-Managementsysteme
(ISO/IEC TS 27006-2: 2021)

Túto technickú špecifikáciu (CEN/TS) schválil CEN 30. októbra 2022 na predbežné používanie.

Obdobie platnosti tejto CEN/TS je obmedzené spočiatku na tri roky. Členovia CEN a CENELEC budú po dvoch rokoch požiadaní o predloženie pripomienok súvisiacich najmä s otázkou, či sa má CEN/TS zmeniť na európsku normu.

Členovia CEN a CENELEC sú povinní oznámiť existenciu tejto technickej špecifikácie CEN/TS takým istým spôsobom ako EN a vhodnou formou sprístupniť túto CEN/TS na národnej úrovni. Do konečného rozhodnutia o možnej konverzii CEN/TS na EN je možné ponechať v platnosti (paralelne s CEN/TS) aj rozporné národné normy.

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, Malty, 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

Ref. č. CEN ISO/IEC/TS 27006-2: 2022 SK

Obsah

strana

Európsky predhovor

Text ISO/IEC TS 27006-2: 2021 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako CEN ISO/IEC/TS 27006-2: 2022 technickou komisiou CEN-CENELEC/JTC 13 *Kybernetická bezpečnosť a ochrana údajov*, ktorej sekretariát je v DIN.

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

Akákoľvek spätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov je na webovom sídle CEN a CENELEC.

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, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text ISO/IEC TS 27006-2: 2021 schválil CEN-CENELEC ako CEN ISO/IEC/TS 27006-2: 2022 bez akýchkoľvek modifikácií.

Úvod

Norma ISO/IEC 27006 stanovuje kritériá pre orgány, ktoré vykonávajú audit a certifikáciu systémov manažérstva informačnej bezpečnosti. Ak majú byť takéto orgány akreditované aj ako orgány spĺňajúce normu ISO/IEC 27006 s cieľom vykonávať audit a certifikáciu systémov riadenia bezpečnosti osobných údajov (PIMS) v súlade s normou ISO/IEC 27701: 2019, sú potrebné niektoré dodatočné požiadavky a usmernenia k norme ISO/IEC 27006. Tieto sú uvedené v tomto dokumente.

Text v tomto dokumente sa riadi štruktúrou normy ISO/IEC 27006 a dodatočné špecifické požiadavky a usmernenia týkajúce sa uplatňovania normy ISO/IEC 27006 na certifikáciu PIMS sú označené písmenami „PS".

Hlavným cieľom tohto dokumentu je umožniť akreditačným orgánom účinnejšie zosúladiť uplatňovanie noriem, podľa ktorých sú povinné posudzovať certifikačné orgány.

1 Predmet

Tento dokument špecifikuje požiadavky a poskytuje usmernenie pre orgány, ktoré zabezpečujú audit a certifikáciu systému riadenia bezpečnosti osobných údajov (PIMS) podľa ISO/IEC 27701 v kombinácii s ISO/IEC 27001, okrem požiadaviek obsiahnutých v ISO/IEC 27006 a ISO/IEC 27701. Je určený predovšetkým na podporu akreditácie certifikačných orgánov poskytujúcich certifikáciu PIMS.

Požiadavky obsiahnuté v tomto dokumente musí preukázať z hľadiska spôsobilosti a spoľahlivosti každý, kto poskytuje certifikáciu PIMS a usmernenie obsiahnuté v tomto dokumente poskytuje dodatočný výklad týchto požiadaviek pre každý orgán poskytujúci certifikáciu PIMS.

POZNÁMKA. – Tento dokument sa môže použiť ako dokument s kritériami pre akreditáciu, vzájomné hodnotenie alebo iné audítorské procesy.

2 Normatívne odkazy

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).

ISO/IEC 17021-1 *Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements*. [Posudzovanie zhody. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky.]

ISO/IEC 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.]

ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*. [Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky.]

ISO/IEC 27006: 2015 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.* [Informačné technológie. Bezpečnostné metódy. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti.]

ISO/IEC 27701 *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*. [Bezpečnostné metódy. Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov. Požiadavky a usmernenia.]

ISO/IEC 29100 *Information technology – Security techniques – Privacy framework.* [Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov.]