ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA September 2026

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Opatrenia informačnej bezpečnosti pre odvetvie energetických služieb (ISO/IEC 27019: 2024)**	**STN EN ISO/IEC 27019** 97 4248

Information security, cybersecurity and privacy protection
Information security controls for the energy utility industry

Sécurité de l'information, cybersécurité et protection de la vie privée
Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen für die Energieversorgung

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27019: 2025.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27019 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27019: 2025.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27019 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN EN ISO/IEC 27019 z marca 2026,
ktorá od 1. 3. 2026 nahradila STN EN ISO/IEC 27019 zo septembra 2020 v celom rozsahu.

142957

Národný predhovor

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27019: 2017), ktoré bolo technicky revidované.

Hlavné zmeny sú nasledovné:

- zosúladenie opatrení s organizačnými, personálnymi, fyzickými a technologickými témami, ktoré sú zahrnuté v norme ISO/IEC 27002: 2022;
- „Usmernenia“ a „Ďalšie informácie“ v kapitolách 5 až 8 boli aktualizované, aby sa zabránilo duplicite s normou ISO/IEC 27002: 2022;
- k opatreniam špecifickým pre tento dokument boli pridané atribúty.

Táto STN obsahuje šesť národných poznámok.

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 27002: 2022 prijatá ako STN EN 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

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27019

December 2025

ICS 35.030

Nahrádza EN ISO/IEC 27019: 2020

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Opatrenia informačnej bezpečnosti pre odvetvie energetických služieb (ISO/IEC 27019: 2024)

Information security, cybersecurity and privacy protection
Information security controls for the energy utility industry
(ISO/IEC 27019: 2024)

Sécurité de l'information, cybersécurité et protection de la vie privée
Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie
(ISO/IEC 27019: 2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen für die Energieversorgung
(ISO/IEC 27019: 2024)

Túto európsku normu schválil CEN 7. decembra 2025.

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, 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. EN ISO/IEC 27019: 2025 SK

Obsah

strana

Európsky predhovor

Text ISO/IEC 27019: 2024 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27019: 2025 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 najneskoršie do júna 2026 a národné normy, ktoré sú s ňou v rozpore sa musia zrušiť najneskoršie do júna 2026.

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.

Tento dokument nahrádza EN ISO/IEC 27019: 2020.

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 27019: 2024 schválil CEN-CENELEC ako EN ISO/IEC 27019: 2025 bez akýchkoľvek modifikácií.

Úvod

0.1 Pozadie a kontext

Tento dokument poskytuje usmernenia založené na norme ISO/IEC 27002: 2022 pre riadenie informačnej bezpečnosti pri uplatňovaní na systémy riadenia procesov používané v energetickom priemysle. Cieľom tohto dokumentu je rozšíriť obsah normy ISO/IEC 27002: 2022 o oblasť systémov riadenia procesov a automatizačnej techniky pre energetický priemysel.

Okrem bezpečnostných cieľov a opatrení, ktoré sú stanovené v norme ISO/IEC 27002: 2022, systémy riadenia procesov používané energetickými podnikmi a dodávateľmi energie podliehajú ďalším osobitným požiadavkám. V porovnaní s bežnými prostredím informačných a komunikačných technológií (IKT) (napr. kancelárske informačné technológie, systémy obchodovania s energiou) existujú zásadné a významné rozdiely, pokiaľ ide o vývoj, prevádzku, opravy, údržbu a prevádzkové prostredie systémov riadenia procesov. Okrem toho procesná technológia uvedená v tomto dokumente môže predstavovať integrálnu súčasť kritických infraštruktúr. To znamená, že sú nevyhnutné pre bezpečnú a spoľahlivú prevádzku takýchto infraštruktúr. Tieto rozdiely a charakteristiky by mali byť riadne zohľadnené v procesoch manažérstva systémov riadenia procesov a odôvodňujú samostatné posúdenie v rámci ISO/IEC 27001 a súvisiacich noriem.

Z hľadiska dizajnu a funkcie sú systémy riadenia procesov používané v energetickom priemysle v skutočnosti systémami na spracovanie informácií. Získavajú procesné údaje a monitorujú stav fyzikálnych procesov pomocou senzorov. Systémy potom spracúvajú tieto údaje a generujú opatrenia, ktoré regulujú činnosti pomocou akčných členov. Riadenie a regulácia sú automatické, ale je možný aj manuálny zásah obsluhujúceho personálu. Informačné systémy a systémy na spracovanie informácií sú preto nevyhnutnou súčasťou prevádzkových procesov v energetických podnikoch. Je dôležité, aby sa uplatňovali primerané opatrenia rovnakým spôsobom ako v prípade iných organizačných jednotiek.

Softvérové a hardvérové komponenty (napr. programovateľná logika) založené na štandardnej technológii IKT sa čoraz viac využívajú v prostrediach riadenia procesov a sú tiež zahrnuté v tomto dokumente. Okrem toho sú systémy riadenia procesov v energetickom priemysle čoraz viac prepojené a tvoria komplexné systémy. Riziká vyplývajúce z tohto trendu by sa mali zohľadniť v posúdení rizík.

Informačné systémy a systémy na spracovanie informácií v prostrediach riadenia procesov sú tiež vystavené rastúcemu počtu hrozieb a zraniteľností.

Účinnú informačnú bezpečnosť v oblasti riadenia procesov v energetickom priemysle je možné dosiahnuť zavedením, implementáciou, monitorovaním, revíziou a v prípade potreby zlepšením príslušných opatrení informačnej bezpečnosti stanovených v tomto dokumente s cieľom dosiahnuť konkrétne bezpečnostné a obchodné ciele organizácie. Je dôležité venovať osobitnú pozornosť špeciálnej úlohe energetických podnikov v spoločnosti a ekonomickej nevyhnutnosti bezpečných a spoľahlivých dodávok energie. Celkový úspech kybernetickej bezpečnosti energetického priemyslu je v konečnom dôsledku založený na spoločnom úsilí všetkých zainteresovaných strán (predajcov, dodávateľov, zákazníkov atď.).

0.2 Bezpečnostné hľadiská pre systémy riadenia procesov používané energetickými podnikmi

Požiadavka na všeobecný a celkový rámec informačnej bezpečnosti pre oblasť riadenia procesov v energetickom priemysle vychádza z niekoľkých základných požiadaviek:

a) Zákazníci očakávajú bezpečné a spoľahlivé dodávky energie.

b) Právne požiadavky vyžadujú bezpečnú, spoľahlivú a zabezpečenú prevádzku systémov dodávok energie.

c) Dodávatelia energie vyžadujú informačnú bezpečnosť, aby mohli chrániť svoje obchodné záujmy, uspokojovať potreby zákazníkov a dodržiavať zákonné predpisy.

0.3 Požiadavky na informačnú bezpečnosť

Je nevyhnutné, aby energetické spoločnosti identifikovali svoje bezpečnostné požiadavky. Existujú tri hlavné zdroje bezpečnostných požiadaviek:

a) posúdenie rizík pre organizáciu s prihliadnutím na celkovú obchodnú stratégiu a ciele organizácie. To možno uľahčiť alebo podporiť prostredníctvom posúdenia rizík špecifických pre informačnú bezpečnosť. Výsledkom by malo byť stanovenie opatrení potrebných na zabezpečenie toho, aby zvyškové riziko pre organizáciu spĺňalo jej kritériá prijateľnosti rizika;

b) právne, zákonné, regulačné a zmluvné požiadavky, ktoré má organizácia a jej zainteresované strany (obchodní partneri, poskytovatelia služieb atď.) spĺňať, a ich sociokultúrne prostredie;

c) súbor zásad, cieľov a obchodných požiadaviek pre všetky fázy životného cyklu informácií, ktoré organizácia vyvinula na podporu svojich činností.

POZNÁMKA. – Je dôležité, aby organizácie dodávajúce energiu zabezpečili, že bezpečnostné požiadavky systémov riadenia procesov sú analyzované a primerane pokryté v politikách informačnej bezpečnosti. Analýza požiadaviek a cieľov informačnej bezpečnosti zahŕňa zohľadnenie všetkých relevantných kritérií pre bezpečné dodávky a distribúciu energie, ako napríklad:

- ohrozenie bezpečnosti dodávok energie;
- obmedzenie toku energie;
- postihnutá časť obyvateľstva;
- nebezpečenstvo fyzického zranenia;
- vplyv na iné kritické infraštruktúry;
- vplyv na ochranu osobných údajov;
- finančné dopady.

0.4 Stanovenie opatrení

Po identifikácii bezpečnostných požiadaviek a rizík a prijatí rozhodnutí o tom, ako s rizikami naložiť, sa vyberú a implementujú primerané opatrenia, aby sa zabezpečilo zníženie rizík na prijateľnú úroveň.

Okrem opatrení na riadenie informačnej bezpečnosti, ktoré poskytuje komplexný systém manažérstva informačnej bezpečnosti, tento dokument poskytuje dodatočnú pomoc a opatrenia špecifické pre jednotlivé sektory pre systémy riadenia procesov používané v odvetví energetických služieb, pričom zohľadňuje osobitné požiadavky v týchto prostrediach. V prípade potreby je možné vyvinúť ďalšie opatrenia na riadenie informačnej bezpečnosti na splnenie konkrétnych požiadaviek. Výber opatrení na riadenie informačnej bezpečnosti závisí od rozhodnutí prijatých organizáciou na základe jej vlastných kritérií akceptovateľnosti rizika, možností riešenia rizika a všeobecného prístupu organizácie k riadeniu rizika.

POZNÁMKA. – Môžu sa uplatňovať vnútroštátne a medzinárodné právne predpisy, nariadenia a regulácie.

0.5 Cieľová skupina

Tento dokument je určený osobám zodpovedným za prevádzku systémov riadenia procesov používaných energetickými podnikmi, manažérom informačnej bezpečnosti, dodávateľom, integrátorom systémov a audítorom. Pre túto cieľovú skupinu tento dokument podrobne opisuje základné opatrenia v súlade s cieľmi normy ISO/IEC 27002: 2022 a definuje konkrétne opatrenia pre systémy riadenia procesov v energetickom priemysle, ich podporné systémy a súvisiacu infraštruktúru.

1 Predmet

Tento dokument poskytuje opatrenia informačnej bezpečnosti pre odvetvie energetických služieb na základe normy ISO/IEC 27002: 2022 na účely riadenia a monitorovania výroby alebo generovania, prenosu, skladovania a distribúcie elektrickej energie, plynu, ropy a tepla a na účely opatrení pre súvisiace podporné procesy. Zahŕňa to najmä nasledujúce:

- centrálnu a distribuovanú technológiu riadenia, monitorovania a automatizácie procesov, ako aj informačné systémy používané na ich prevádzku, ako sú programovacie a parametrizačné zariadenia;
- digitálne regulátory a automatizačné komponenty, ako sú riadiace a prevádzkové zariadenia alebo programovateľné logické automaty (PLC)*), vrátane digitálnych senzorov a akčných členov;
- všetky ďalšie podporné informačné systémy používané v oblasti riadenia procesov, napr. na doplňujúce úlohy vizualizácie údajov a na účely riadenia, monitorovania, archivácie údajov, logovania histórie, podávania správ a dokumentácie;
- komunikačné technológie používané v oblasti riadenia procesov, napr. siete, telemetria, aplikácie diaľkového ovládania a technológie diaľkového ovládania;
- komponenty pokročilej meracej infraštruktúry (AMI)**), napr. inteligentné meracie zariadenia;
- meracie zariadenia, napr. na meranie emisií;
- digitálne ochranné a bezpečnostné systémy, napr. ochranné relé, bezpečnostné PLC, núdzové regulačné mechanizmy;
- systémy manažérstva energie, napr. pre distribuované energetické zdroje (DER)***), infraštruktúry pre elektrické nabíjanie a pre súkromné domácnosti, obytné budovy alebo priemyselné zariadenia zákazníkov;
- distribuované komponenty prostredí inteligentných sietí, napr. v energetických sieťach, v súkromných domácnostiach, obytných budovách alebo priemyselných zariadeniach zákazníkov;
- všetok softvér, firmvér a aplikácie inštalované na vyššie uvedených systémoch, napr. aplikácie systému manažérstva distribúcie (DMS)****) alebo systémy riadenia výpadkov (OMS)*****);
- akékoľvek priestory, v ktorých sa nachádzajú vyššie uvedené zariadenia a systémy;
- systémy diaľkovej údržby pre vyššie uvedené systémy.

Tento dokument sa nevzťahuje na oblasť riadenia procesov jadrových zariadení. Táto oblasť je upravená normou IEC 63096.

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 27002: 2022 *Information security, cybersecurity and privacy protection – Information security controls.* [Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Opatrenia informačnej bezpečnosti.]

*) NÁRODNÁ POZNÁMKA 1. – PLC – angl. programmable logic controllers.

**) NÁRODNÁ POZNÁMKA 2. – AMI – angl. advanced metering infrastructure.

***) NÁRODNÁ POZNÁMKA 3. – DER – angl. distributed energy resources.

****) NÁRODNÁ POZNÁMKA 4. –DMS – angl. distribution management system.

*****) NÁRODNÁ POZNÁMKA 5. – OMS – angl. outage management systems.