SLOVENSKI STANDARD

SIST EN ISO/IEC 27001

november 2023

Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Sistemi vodenja informacijske varnosti – Zahteve (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2022)

ICS 03.100.70; 35.030

Referenčna oznaka
SIST EN ISO/IEC 27001:2023 (sl)

Nadaljevanje na straneh ii ter od 2 do 25

NACIONALNI UVOD

Standard SIST EN ISO/IEC 27001 (sl), Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Sistemi vodenja informacijske varnosti – Zahteve (ISO/IEC 27001:2022), 2023, ima status slovenskega standarda in je enakovreden evropskemu standardu EN ISO/IEC 27001 (en, fr, de), Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022), 2023.

NACIONALNI PREDGOVOR

Besedilo standarda EN ISO/IEC 27001:2023 je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija. Slovenski standard SIST EN ISO/IEC 27001:2023 je prevod angleškega besedila evropskega standarda EN ISO/IEC 27001:2023. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvirni evropski standard v angleškem jeziku. Slovensko izdajo standarda je pripravil SIST/TC ITC Informacijska tehnologija.

Odločitev za privzem tega standarda je dne 27. 1. 2025 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZE S STANDARDI

S privzemom tega evropskega standarda veljajo za omenjeni namen referenčnih standardov vsi standardi, navedeni v izvirniku, razen tistih, ki so že sprejeti v nacionalno standardizacijo:

SIST EN ISO/IEC 27000	Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Pregled in izrazje

OSNOVA ZA IZDAJO STANDARDA

- privzem standarda EN ISO/IEC 27001:2023

PREDHODNA IZDAJA

- SIST ISO/IEC 27001:2017, Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve (ISO/IEC 27001:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015)

OPOMBE

- Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST EN ISO/IEC 27001:2023 to pomeni "slovenski standard".
- Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.
- Ta nacionalni dokument je enakovreden EN ISO/IEC 27001:2023 in je objavljen z dovoljenjem

  CEN-CENELEC
  Upravni center
  Rue de la Science 23
  B-1040 Bruselj

- This national document is identical with EN ISO 27001:2023 and is published with the permission of

  CEN-CENELEC
  Management Centre
  Rue de la Science 23
  B-1040 Brussels

EVROPSKI STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

julij 2023

ICS 03.100.70; 35.030

Slovenska izdaja

Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Sistemi vodenja informacijske varnosti – Zahteve (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)	Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2022)	Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022)

Ta evropski standard je CEN sprejel 23. julija 2023.

Člani CEN in CENELEC morajo izpolnjevati notranje predpise CEN/CENELEC, s katerimi je predpisano, da mora biti ta standard brez kakršnihkoli sprememb sprejet kot nacionalni standard. Seznami najnovejših izdaj teh nacionalnih standardov in njihovi bibliografski podatki so na zahtevo na voljo pri Upravnem centru CEN-CENELEC ali kateremkoli članu CEN in CENELEC.

Ta evropski standard obstaja v treh uradnih izdajah (angleški, francoski, nemški). Izdaje v drugih jezikih, ki jih člani CEN in CENELEC na lastno odgovornost prevedejo in izdajo ter prijavijo pri Upravnem centru CEN-CENELEC, veljajo kot uradne izdaje.

Člani CEN in CENELEC so nacionalni organi za standarde in nacionalni elektrotehniški odbori Avstrije, Belgije, Bolgarije, Cipra, Češke republike, Danske, Estonije, Finske, Francije, Grčije, Hrvaške, Irske, Islandije, Italije, Latvije, Litve, Luksemburga, Madžarske, Malte, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Republike Severna Makedonija, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije in Združenega kraljestva.

CEN-CENELEC
CEN-CENELEC Upravni center
Rue de la Science 23, B-1040 Bruselj

VSEBINA **Stran**

Evropski predgovor

Besedilo standarda ISO/IEC 27001:2022 je pripravil tehnični odbor ISO/IEC JTC 1 "Informacijska tehnologija" Mednarodne organizacije za standardizacijo (ISO) in ga je kot EN ISO/IEC 27001:2023 sprejel tehnični odbor CEN-CENELEC/JTC 13 "Kibernetska varnost in varstvo podatkov", katerega sekretariat vodi DIN.

Ta evropski standard mora z objavo istovetnega besedila ali z razglasitvijo dobiti status nacionalnega standarda najpozneje do januarja 2024, nacionalne standarde, ki so v nasprotju s tem standardom, pa je treba razveljaviti najpozneje do januarja 2024.

Opozoriti je treba na možnost, da je lahko nekaj elementov tega dokumenta predmet patentnih pravic. CEN-CENELEC ni odgovoren za identificiranje katerekoli ali vseh takih patentnih pravic.

Ta dokument nadomešča EN ISO/IEC 27001:2017.

Uporabnik naj vse povratne informacije ali vprašanja o tem dokumentu posreduje nacionalnemu organu za standarde v svoji državi. Celoten seznam teh organov je na voljo na spletnih straneh CEN in CENELEC.

V skladu z notranjimi predpisi CEN-CENELEC morajo ta evropski standard obvezno uvesti nacionalne organizacije za standardizacijo naslednjih držav: Avstrije, Belgije, Bolgarije, Cipra, Češke republike, Danske, Estonije, Finske, Francije, Grčije, Hrvaške, Irske, Islandije, Italije, Latvije, Litve, Luksemburga, Madžarske, Malte, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Republike Severna Makedonija, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije in Združenega kraljestva.

Razglasitvena objava

Besedilo standarda ISO/IEC 27001:2022 je CEN odobril kot EN ISO/IEC 27001:2023 brez sprememb.

Vsebina **Stran**

Predgovor k mednarodnemu standardu

ISO (Mednarodna organizacija za standardizacijo) in IEC (Mednarodna elektrotehniška komisija) tvorita specializiran sistem za svetovno standardizacijo. Nacionalni organi, ki so člani ISO ali IEC, sodelujejo pri pripravi mednarodnih standardov prek tehničnih odborov, ki jih za obravnavanje določenih strokovnih področij ustanovi ustrezna organizacija. Tehnični odbori ISO in IEC sodelujejo na področjih skupnega interesa. Pri delu sodelujejo tudi druge mednarodne, vladne in nevladne organizacije, povezane z ISO in IEC.

Postopki, uporabljeni pri pripravi tega dokumenta, in predvideni postopki za njegovo vzdrževanje so opisani v 1. delu Direktiv ISO/IEC. Posebna pozornost naj se nameni različnim kriterijem odobritve, potrebnim za različne vrste dokumentov. Ta dokument je bil zasnovan v skladu z uredniškimi pravili 2. dela Direktiv ISO/IEC (glej www.iso.org/directives ali www.iec.ch/members_experts/refdocs).

Opozoriti je treba na možnost, da bi lahko bil kateri od elementov tega dokumenta predmet patentnih pravic. ISO in IEC nista odgovorna za identificiranje katerekoli ali vseh takih patentnih pravic. Podrobnosti o morebitnih patentnih pravicah, identificiranih med pripravo tega dokumenta, bodo navedene v uvodu in/ali na seznamu patentnih izjav, ki jih je prejela organizacija ISO (glej www.iso.org/patents), ali na seznamu patentnih izjav, ki jih je prejela organizacija IEC (glej https://patents.iec.ch).

Vsakršna trgovska imena, uporabljena v tem dokumentu, so informacije za uporabnike in ne pomenijo podpore blagovni znamki.

Za razlago prostovoljne narave standardov, pomena specifičnih pojmov in izrazov ISO, povezanih z ugotavljanjem skladnosti, ter informacij o tem, kako ISO upošteva načela Svetovne trgovinske organizacije (WTO) v Tehničnih ovirah pri trgovanju (TBT), glej naslednjo povezavo www.iso.org/iso/foreword.html. Pri IEC glej povezavo www.iec.ch/understanding-standards.

Ta dokument je pripravil združeni tehnični odbor ISO/IEC JTC 1, *Informacijska tehnologija,* pododbor SC 27 *Informacijska varnost, kibernetska varnost in varstvo zasebnosti*.

Ta tretja izdaja preklicuje in nadomešča drugo izdajo (ISO/IEC 27001:2013), ki je tehnično revidirana. Vsebuje tudi tehnična popravka ISO/IEC 27001:2013/Cor 1:2014 in ISO/IEC 27001:2013/Cor 2:2015.

Glavne spremembe so naslednje:

– besedilo je bilo usklajeno s harmonizirano strukturo standardov za sisteme vodenja in ISO/IEC 27002:2022.

Uporabnik naj vse povratne informacije ali vprašanja o tem dokumentu posreduje nacionalnemu organu za standarde v svoji državi. Celoten seznam teh organov je na voljo na naslovih www.iso.org/members.html in www.iec.ch/national-committees.

Uvod

0.1 Splošno

Ta dokument je bil pripravljen, da zagotovi zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema vodenja informacijske varnosti. Privzem sistema vodenja informacijske varnosti je strateška odločitev za organizacijo. Na vzpostavitev in izvedbo sistema vodenja informacijske varnosti organizacije vplivajo potrebe in cilji organizacije, varnostne zahteve, uporabljeni organizacijski procesi ter velikost in struktura organizacije. Vsi ti dejavniki, ki vplivajo na sistem, se bodo po pričakovanjih s časom spreminjali.

Sistem vodenja informacijske varnosti ohranja zaupnost, celovitost in razpoložljivost informacij z uporabo procesa za obvladovanje tveganja ter zainteresiranim stranem vzbuja zaupanje, da se tveganja ustrezno obvladujejo.

Pomembno je, da je sistem vodenja informacijske varnosti del procesov organizacije in splošne strukture vodenja in je integriran z njimi ter da je informacijska varnost sprejeta pri zasnovi procesov, informacijskih sistemov in kontrol. Pričakuje se, da bo izvajanje sistema vodenja informacijske varnosti skladno s potrebami organizacije.

Ta dokument lahko uporabljajo notranje ali zunanje stranke za ocenjevanje sposobnosti organizacije izpolnjevati lastne zahteve informacijske varnosti.

Vrstni red predstavitve zahtev v tem dokumentu ne odraža njihovega pomena ali nakazuje vrstnega reda, v katerem naj bi se izvedle. Elementi na seznamu so oštevilčeni zgolj za namene sklicevanja.

Standard ISO/IEC 27000 podaja pregled in izrazje sistemov vodenja informacijske varnosti, pri čemer se sklicuje na skupino standardov za sisteme vodenja informacijske varnosti (vključno s standardi ISO/IEC 27003[2], ISO/IEC 27004[3] in ISO/IEC 27005[4]) s povezanimi izrazi in definicijami.

0.2 Združljivost z drugimi standardi za sisteme vodenja

Ta dokument uporablja strukturo visoke ravni, enake naslove podtočk, enako besedilo, splošne izraze in temeljne definicije iz dodatka SL k Direktivam ISO/IEC, 1. del, konsolidirana priloga ISO, zato ohranja združljivost z drugimi standardi za sisteme vodenja, ki so sprejeli dodatek SL.

Ta splošni pristop iz dodatka SL bo koristil tistim organizacijam, ki so izbrale vzpostavitev enotnega sistema vodenja, ki izpolnjuje zahteve iz dveh ali več standardov za sisteme vodenja.

Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Sistemi vodenja informacijske varnosti – Zahteve

1 Področje uporabe

Ta dokument določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema vodenja informacijske varnosti v okviru organizacije. Ta dokument zajema tudi zahteve za ocenjevanje in obravnavanje tveganj informacijske varnosti, ki so prilagojene potrebam organizacije. Zahteve, določene v tem dokumentu, so generične in so namenjene uporabi v vseh organizacijah ne glede na vrsto, velikost ali naravo. Izključevanje katerekoli zahteve, določene v točkah 4 do 10, ni sprejemljivo, kadar organizacija zagotavlja skladnost s tem dokumentom.

2 Zveze s standardi

Naslednji dokumenti so v besedilu navedeni na način, da njihov del ali celotna vsebina predstavlja zahteve tega dokumenta. Pri datiranih sklicevanjih se uporablja zgolj navedena izdaja. Pri nedatiranih sklicevanjih se uporablja zadnja izdaja navedenega dokumenta (vključno z dopolnili).

ISO/IEC 27000, Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Pregled in izrazje

3 Izrazi in definicije

V tem dokumentu so uporabljeni izrazi in definicije, ki so podani v standardu ISO/IEC 27000.
ISO in IEC hranita terminološke podatkovne zbirke za uporabo pri standardizaciji na naslednjih naslovih:

– Platforma za spletno brskanje ISO: na voljo na https://www.iso.org/obp

– IEC Electropedia: na voljo na spletnem mestu https://www.electropedia.org/

4 Kontekst organizacije

4.1 Razumevanje organizacije in njenega konteksta

Organizacija mora določiti zunanja in notranja vprašanja, ki so pomembna za njen namen ter vplivajo na njeno sposobnost doseganja pričakovanega(-ih) rezultata(-ov) njenega sistema vodenja informacijske varnosti.

OPOMBA: Določanje teh vprašanj se nanaša na opredelitev zunanjega in notranjega konteksta organizacije iz točke 5.4.1 standarda ISO 31000:2018[5].

4.2 Razumevanje potreb in pričakovanj zainteresiranih strani

Organizacija mora določiti:

a) zainteresirane strani, ki so pomembne za sistem vodenja informacijske varnosti,

b) ustrezne zahteve teh zainteresiranih strani,

c) katere od teh zahtev bodo obravnavane v okviru sistema vodenja informacijske varnosti.

OPOMBA: Zahteve zainteresiranih strani lahko vključujejo zahteve zakonodaje in predpisov ter pogodbene obveznosti.

4.3 Določitev obsega sistema vodenja informacijske varnosti

Organizacija mora določiti meje in uporabnost sistema vodenja informacijske varnosti za opredelitev njegovega obsega.

Organizacija pri določanju tega obsega upošteva: