
Informacijska varnost, kibernetika varnost in varstvo zasebnosti – Kontrole informacijske varnosti (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité de l'information (ISO/IEC 27002:2022)

Document Preview

[SIST EN ISO/IEC 27002:2022](https://standards.iteh.ai/catalog/standards/sist/5a6701a3-64b3-41fd-bebd-37a6b9c51eb2/sist-en-iso-iec-27002-2022)

<https://standards.iteh.ai/catalog/standards/sist/5a6701a3-64b3-41fd-bebd-37a6b9c51eb2/sist-en-iso-iec-27002-2022>

ICS 03.100.70; 35.030

Referenčna oznaka
SIST EN ISO/IEC 27002:2022 (sl)

Nadaljevanje na straneh II ter od 2 do 171

NACIONALNI UVOD

Standard SIST EN ISO/IEC 27002 (sl), Informacijska varnost, kibernetika varnost in varstvo zasebnosti – Kontrole informacijske varnosti (ISO/IEC 27002:2022), 2022, ima status slovenskega standarda in je enakovreden evropskemu standardu EN ISO/IEC 27002 (en, fr, de), Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022), 2022.

NACIONALNI PREDGOVOR

Besedilo standarda EN ISO/IEC 27002:2022 je pripravil združeni tehnični odbor Evropskega komiteja za standardizacijo CEN-CENELEC/JTC 13 Kibernetika varnost in varstvo podatkov. Slovenski standard SIST EN ISO/IEC 27002:2022 je prevod angleškega besedila evropskega standarda EN ISO/IEC 27002:2022. 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 29. novembra 2022 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

- privzem standarda EN ISO/IEC 27002:2022

PREDHODNA IZDAJA

- SIST EN ISO/IEC 27002:2017, Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti (ISO/IEC 27002:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015)

OPOMBE

- Povsod, kjer se v besedilu standarda uporablja izraz "evropski standard", v SIST EN ISO/IEC 27002:2022 to pomeni "slovenski standard".
- Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.
- Ta nacionalni dokument je enakovreden EN ISO/IEC 27002:2022 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 27002:2022 and is published with the permission of

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

Slovenska izdaja

**Informacijska varnost, kibernetska varnost in varstvo zasebnosti –
Kontrole informacijske varnosti (ISO/IEC 27002:2022)**

Information security, cybersecurity
and privacy protection –
Information security controls
(ISO/IEC 27002:2022)

Sécurité de l'information,
cybersécurité et protection de la
vie privée – Moyens de maîtrise de
l'information (ISO/IEC 27002:2022)

Informationssicherheit,
Cybersicherheit und Schutz der
Privatsphäre –
Informationssicherheitsmaßnahmen
(ISO/IEC 27002:2022)

Ta evropski standard je CEN sprejel 30. oktobra 2022.

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.....	3
-------------------------	---

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27002:2022](https://standards.iteh.ai/catalog/standards/sist/5a6701a3-64b3-41fd-bebd-37a6b9c51eb2/sist-en-iso-iec-27002-2022)

<https://standards.iteh.ai/catalog/standards/sist/5a6701a3-64b3-41fd-bebd-37a6b9c51eb2/sist-en-iso-iec-27002-2022>

Evropski predgovor

Besedilo standarda ISO/IEC 27002:2022 je pripravil tehnični odbor ISO/IEC JTC 1 "Informacijska tehnologija" Mednarodne organizacije za standardizacijo (ISO) in ga je kot EN ISO/IEC 27002:2022 sprejel tehnični odbor CEN-CENELEC/JTC 13 "Kibernetika, 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 maja 2023, nacionalne standarde, ki so v nasprotju s tem standardom, pa je treba razveljaviti najpozneje do maja 2023.

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 27002:2017.

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 mestih 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.

iteh Standards
(<https://standards.iteh.ai>)
Razglasitvena objava

Besedilo standarda ISO/IEC 27002:2022 je CEN-CENELEC odobril kot EN ISO/IEC 27002:2022 brez sprememb.

SIST EN ISO/IEC 27002:2022

<https://standards.iteh.ai/catalog/standards/sist/5a6701a3-64b3-41fd-bebd-37a6b9c51eb2/sist-en-iso-iec-27002-2022>

Vsebina	Stran
Predgovor k mednarodnemu standardu.....	7
Uvod.....	8
1 Področje uporabe.....	11
2 Zveze s standardi.....	11
3 Izrazi, definicije in kratice.....	11
3.1 Izrazi in definicije.....	11
3.2 Kratice.....	16
4 Struktura tega dokumenta.....	17
4.1 Točke.....	17
4.2 Teme in atributi.....	17
4.3 Ureditev kontrol.....	19
5 Organizacijske kontrole.....	19
5.1 Politike za informacijsko varnost.....	19
5.2 Vloge in odgovornosti na področju informacijske varnosti.....	21
5.3 Razmejitev dolžnosti.....	22
5.4 Odgovornosti vodstva.....	23
5.5 Stik s pristojnimi organi.....	24
5.6 Stik s specifičnimi interesnimi skupinami.....	25
5.7 Obveščanje o grožnjah.....	25
5.8 Informacijska varnost pri vodenju projektov.....	27
5.9 Seznam informacij in drugih povezanih sredstev.....	28
5.10 Sprejemljiva uporaba informacij in drugih povezanih sredstev.....	30
5.11 Vračilo sredstev.....	31
5.12 Razvrstitev informacij.....	32
5.13 Označevanje informacij.....	34
5.14 Prenos informacij.....	35
5.15 Nadzor dostopa.....	37
5.16 Upravljanje identitete.....	39
5.17 Informacije za avtentikacijo.....	40
5.18 Pravice dostopa.....	42
5.19 Informacijska varnost v odnosih z dobavitelji.....	44
5.20 Obravnavanje informacijske varnosti v dogovorih z dobavitelji.....	46
5.21 Vodenje informacijske varnosti v dobavni verigi informacijske in komunikacijske tehnologije (IKT).....	48
5.22 Spremljanje, pregled in upravljanje sprememb storitev dobaviteljev.....	50
5.23 Informacijska varnost za uporabo storitev v oblaku.....	51
5.24 Načrtovanje in priprava vodenja informacijskih varnostnih incidentov.....	53
5.25 Ocenjevanje informacijskih varnostnih dogodkov in odločanje o njih.....	55
5.26 Odziv na informacijske varnostne incidente.....	56

5.27	Učenje iz informacijskih varnostnih incidentov	57
5.28	Zbiranje dokazov	58
5.29	Informacijska varnost med motnjo	59
5.30	Pripravljenost informacijske in komunikacijske tehnologije za neprekinjeno poslovanje	59
5.31	Pravne, zakonske, regulativne in pogodbene zahteve	61
5.32	Pravice intelektualne lastnine	63
5.33	Zaščita zapisov	64
5.34	Zasebnost in zaščita osebno določljivih podatkov	65
5.35	Neodvisni pregled informacijske varnosti	66
5.36	Skladnost s politikami, pravili in standardi informacijske varnosti	67
5.37	Dokumentirani postopki delovanja	68
6	Kontrole oseb	69
6.1	Preverjanje	69
6.2	Določila in pogoji za zaposlitev	71
6.3	Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti	72
6.4	Disciplinski proces	73
6.5	Odgovornosti po prekinitvi ali spremembi zaposlitve	74
6.6	Dogovori o zaupnosti ali nerazkrivanju	75
6.7	Delo na daljavo	76
6.8	Poročanje o informacijskem varnostnem dogodku	78
7	Fizične kontrole	79
7.1	Varovanje fizičnih meja območja	79
7.2	Fizični vstop	80
7.3	Varovanje pisarn, sob in naprav	81
7.4	Nadzor fizične varnosti	82
7.5	Zaščita pred fizičnimi in okoljskimi grožnjami	83
7.6	Delo na varovanih območjih	84
7.7	Načelo čiste mize in praznega zaslona	85
7.8	Namestitev in zaščita opreme	86
7.9	Varnost sredstev zunaj prostorov organizacije	87
7.10	Nosilci za shranjevanje podatkov/informacij	88
7.11	Podporna oskrba	90
7.12	Varnost ožičenja	91
7.13	Vzdrževanje opreme	92
7.14	Varna odstranitev ali ponovna uporaba opreme	93
8	Tehnološke kontrole	94
8.1	Končne naprave uporabnika	94
8.2	Posebne pravice dostopa	96
8.3	Omejitev dostopa do informacij	97
8.4	Dostop do izvirne kode	99