SLOVENSKI STANDARD

SIST ISO/IEC 27003

november 2018

Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Smernice

Information technology – Security techniques – Information security management systems – Guidance

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Lignes directrices

ICS 03.100.70; 35.030

Referenčna oznaka
SIST ISO/IEC 27003:2018 (sl)

Nadaljevanje na straneh 2 do 52

NACIONALNI UVOD

Standard SIST ISO/IEC 27003 (sl), Informacijska tehnologija – Varnostne tehnike – Sistemi vodenja informacijske varnosti – Smernice, 2018, ima status slovenskega standarda in je istoveten z mednarodnim standardom ISO/IEC 27003 (en, fr, de), Information technology – Security techniques – Information security management systems – Guidance, 2017.

NACIONALNI PREDGOVOR

Besedilo standarda ISO/IEC 27003:2017 je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija. Slovenski standard SIST ISO/IEC 27003:2018 je prevod angleškega besedila mednarodnega standarda ISO/IEC 27003:2017. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvirni mednarodni standard v angleškem jeziku. Slovensko izdajo standarda je pripravil SIST/TC ITC Informacijska tehnologija.

Odločitev za privzem tega standarda je dne 1. novembra 2018 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

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

SIST EN ISO/IEC 27000:2017, Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazje

ISO/IEC 27001:2013, Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

OSNOVA ZA IZDAJO STANDARDA

- privzem standarda ISO/IEC 27003:2017

PREDHODNA IZDAJA

- SIST ISO/IEC 27003:2011, Informacijska tehnologija – Varnostne tehnike – Smernice za izvedbo sistema upravljanja informacijske varnosti

OPOMBE

- Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27003:2018 to pomeni “slovenski standard”.

- Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

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. Na področju informacijske tehnologije sta ISO in IEC ustanovila združeni tehnični odbor ISO/IEC JTC 1.

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).

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).

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 spoštuje načela Svetovne trgovinske organizacije (WTO) v Tehničnih ovirah pri trgovanju (TBT), glej naslednji naslov URL: www.iso.org/iso/foreword.html.

Ta dokument je pripravil združeni tehnični odbor ISO/IEC JTC 1, *Informacijska tehnologija,* pododbor *SC 27, Varnostne tehnike IT.*

Ta druga izdaja standarda ISO/IEC 27003 razveljavlja in nadomešča prvo izdajo (ISO/IEC 27003:2010) ter vključuje manjše popravke.

Glavne spremembe glede na predhodno izdajo so naslednje:

– področje uporabe in naslov sta spremenjena, da vključujeta razlago in smernice glede zahtev standarda ISO/IEC 27001:2013, ne predhodne izdaje (ISO/IEC 27001:2005),

– struktura je zdaj usklajena s strukturo standarda ISO/IEC 27001:2013, ki uporabniku omogoča lažjo uporabo skupaj s tem standardom,

– predhodna izdaja je sledila projektnemu pristopu z zaporedjem aktivnosti. Ta izdaja pa zagotavlja smernice v zvezi z zahtevami ne glede na vrstni red, v katerem se izvajajo.

Uvod

Ta dokument podaja smernice glede zahtev za sistem vodenja informacijske varnosti (ISMS), kot je določeno v standardu ISO/IEC 27001, in vključuje priporočila ("naj"), možnosti ("je mogoče") in dovoljenja ("se lahko") v zvezi z njimi. Namen tega dokumenta ni zagotovitev splošnih smernic glede vseh vidikov informacijske varnosti.

Točke od 4 do 10 v tem dokumentu odražajo strukturo standarda ISO/IEC 27001:2013.

Ta dokument ne dodaja nobenih novih zahtev za sistem vodenja informacijske varnosti ter z njim povezanih izrazov in definicij. Organizacije se naj za zahteve in definicije sklicujejo na standarda ISO/IEC 27001 in ISO/IEC 27000. Organizacije, ki izvajajo sistem vodenja informacijske varnosti, niso dolžne upoštevati smernic iz tega dokumenta.

Sistem vodenja informacijske varnosti poudarja pomen naslednjih faz:

– razumevanje potreb organizacije in potrebe po vzpostavitvi informacijske varnostne politike in določitvi ciljev informacijske varnosti,

– ocenjevanje tveganj organizacije, povezanih z informacijsko varnostjo,

– izvajanje in upravljanje procesov informacijske varnosti, kontrol in drugih ukrepov za obravnavo tveganj,

– spremljanje in pregledovanje delovanja in uspešnosti sistema vodenja informacijske varnosti; in

– izvajanje nenehnega izboljševanja.

Podobno kot drugi sistemi vodenja tudi sistem vodenja informacijske varnosti vključuje naslednje ključne komponente:

a) politiko,

b) osebe z določeno odgovornostjo,

c) procese vodenja, povezane s/z:

   1) oblikovanjem politike,

   2) ozaveščenostjo in zagotavljanjem kompetentnosti,

   3) načrtovanjem,

   4) izvajanjem,

   5) upravljanjem,

   6) oceno delovanja,

   7) vodstvenim pregledom; in

   8) izboljšanjem; ter

d) dokumentirane informacije.

Sistem vodenja informacijske varnosti zajema dodatne ključne komponente, kot sta:

e) ocenjevanje tveganj informacijske varnosti; in

f) obravnavanje tveganj informacijske varnosti, vključno z določanjem in izvajanjem kontrol.

Ta dokument je splošen in je namenjen uporabi v vseh organizacijah ne glede na vrsto, velikost ali naravo. Organizacija naj ugotovi, kateri del teh smernic velja zanjo glede na njen ustrezen organizacijski kontekst (glej točko 4 v ISO/IEC 27001:2013).

Nekatere smernice, na primer, so lahko ustreznejše za večje organizacije, medtem ko so za zelo

majhne organizacije (npr. z manj kot 10 osebami) nekatere smernice lahko nepotrebne ali neustrezne.

Opisi točk od 4 do 10 so strukturirani na naslednji način:

- **zahtevana aktivnost**: predstavlja ključne aktivnosti, ki so zahtevane v ustrezni podtočki standarda ISO/IEC 27001,
- **razlaga**: pojasnjuje, kaj pomenijo zahteve standarda ISO/IEC 27001,
- **smernice**: zagotavljajo podrobnejše ali podporne informacije za izvajanje "zahtevane aktivnosti", vključno s primeri za izvajanje; in
- **druge informacije**: navaja druge informacije, ki ji je mogoče upoštevati.

ISO/IEC 27003, ISO/IEC 27004 in ISO/IEC 27005 tvorijo nabor dokumentov za podporo in podajanje smernic za ISO/IEC 27001:2013. Med njimi je ISO/IEC 27003 osnoven in celovit dokument, ki podaja smernice za vse zahteve standarda ISO/IEC 27001, vendar ne vključuje podrobnih opisov v zvezi s "spremljanjem, merjenjem, analizo in vrednotenjem" ter obvladovanjem tveganj informacijske varnosti. ISO/IEC 27004 in ISO/IEC 27005 se osredotočata na določene vsebine in podajata podrobnejše smernice za "spremljanje, merjenje, analizo in vrednotenje" ter obvladovanje tveganj informacijske varnosti.

V ISO/IEC 27001 je več sklicevanj na izključen način na dokumentirane informacije. Vseeno pa lahko organizacija zadrži dodatne dokumentirane informacije, ki jih določi kot potrebne za uspešnost svojega sistema vodenja kot del odgovora na točko 7.5.1 b) standarda ISO/IEC 27001:2013. V teh primerih se v dokumentu uporablja navedba "dokumentirane informacije o tej aktivnosti in njenem rezultatu so obvezne samo v obliki ter obsegu, ki ju organizacija določi kot potrebna za uspešnost svojega sistema vodenja (glej 7.5.1 b) v ISO/IEC 27001:2013) ".