S L O V E N S K I
S T A N D A R D

SIST EN ISO/IEC 27001

julij 2017

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

Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

ICS 03.100.70; 35.030

Referenčna oznaka
SIST EN ISO/IEC 27001:2017 (sl)

Nadaljevanje na straneh II in od 1 do 30

NACIONALNI UVOD

Standard SIST EN ISO/IEC 27001 (sl, en), Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve (ISO/IEC 27001:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015), 2017, ima status slovenskega standarda in je enakovreden evropskemu standardu EN ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015), 2017.

NACIONALNI PREDGOVOR

Besedilo standarda EN ISO/IEC 27001:2017 je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija. Slovenski standard SIST EN ISO/IEC 27001:2017 je prevod angleškega besedila evropskega standarda EN ISO/IEC 27001:2017. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvirni evropski standard v angleškem jeziku. Slovensko-angleško izdajo standarda je pripravil SIST/TC ITC Informacijska tehnologija.

Odločitev za privzem tega standarda je dne 19. maja 2017 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda EN ISO/IEC 27001:2017

PREDHODNA IZDAJA

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

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v v SIST EN ISO/IEC 27001:2017 to pomeni "slovenski standard".
– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.
– Ta nacionalni dokument je istoveten EN ISO/IEC 27001:2017 in je objavljen z dovoljenjem

CEN
Avenue Marnix 17
1050 Bruselj
Belgija

This national document is identical with EN ISO/IEC 27001:2017 and is published with the permission of

CEN
Avenue Marnix 17
1050 Bruxelles
Belgium

EVROPSKI STANDARD
EUROPEAN STANDARD
EUROPÄISCHE NORM
NORME EUROPÉENNE

EN ISO/IEC 27001

februar 2017

ICS: 03.100.70; 35.030

Slovenska izdaja

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

Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Ta evropski standard je CEN sprejel 26. januarja 2017.

Člani CEN in CENELEC morajo izpolnjevati notranje predpise CEN/CENELEC, s katerimi je predpisano, da mora biti ta standard brez kakršnih koli sprememb sprejet ko nacionalni standard. Seznami najnovejših izdaj teh nacionalnih standardov in njihovi bibliografski podatki so na zahtevo na voljo pri Upravnem centru CEN-CENELEC ali pri 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 Avstrije, Belgije, Bolgarije, Cipra, Češke republike, Danske, Estonije, Finske, Francije, Grčije, Hrvaške, Irske, Islandije, Italije, Latvije, Litve, Luksemburga, Madžarske, Malte, Nekdanje jugoslovanske republike Makedonije, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije, in Združenega kraljestva.

CEN-CENELEC
Evropski komite za standardizacijo
European Committee for Standardization
Europäisches Komitee für Normung
Comité Européen de Normalisation

Upravni center CEN-CENELEC: Avenue Marnix 17, B-1000 Bruselj

Ref. oznaka: EN ISO/IEC 27001:2017 E

Vsebina **Stran**

Predgovor k evropskemu standardu

Besedilo standarda ISO/IEC 27001:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015, je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija in je bil sprejet kot EN ISO/IEC 27001:2017

Ta evropski standard mora z objavo istovetnega besedila ali z razglasitvijo dobiti status nacionalnega standarda najpozneje do avgusta 2017, nacionalne standarde, ki so v nasprotju s tem standardom, pa je treba umakniti najpozneje do avgusta 2017.

Opozoriti je treba na možnost, da je lahko nekaj elementov tega dokumenta predmet patentnih pravic. CEN [in/ali CENELEC] ne prevzema odgovornosti za identifikacijo katerih koli ali vseh takih patentnih pravic.

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, Nekdanje jugoslovanske republike Makedonije, Nemčije, Nizozemske, Norveške, Poljske, Portugalske, Romunije, Slovaške, Slovenije, Srbije, Španije, Švedske, Švice, Turčije, in Združenega kraljestva.

Razglasitvena objava

Besedilo mednarodnega standarda ISO/IEC 27001:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015, je CEN odobril kot evropski standard EN ISO/IEC 27001:2017 brez kakršnekoli spremembe.

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 vzpostavila združeni tehnični odbor ISO/IEC JTC 1.

Mednarodni standardi so pripravljeni v skladu s pravili, podanimi v 2. delu Direktiv ISO/IEC.

Glavna naloga tehničnih odborov je priprava mednarodnih standardov. Osnutki mednarodnih standardov, ki jih sprejmejo tehnični odbori, se pošljejo vsem članom v glasovanje. Za objavo mednarodnega standarda je treba pridobiti soglasje najmanj 75 odstotkov članov, ki se udeležijo glasovanja.

Opozoriti je treba na možnost, da je lahko nekaj elementov tega mednarodnega standarda predmet patentnih pravic. ISO in IEC ne prevzemata odgovornosti za prepoznavanje katerih koli ali vseh takih patentnih pravic.

ISO/IEC 27001 je pripravil združeni tehnični odbor ISO/IEC JTC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

Druga izdaja preklicuje in nadomešča prvo izdajo (ISO/IEC 27001:2005), ki je tehnično revidirana.

0 Uvod

0.1 Splošno

Ta mednarodni standard je bil pripravljen, da zagotovi zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti. Privzem sistema upravljanja informacijske varnosti je strateška odločitev za organizacijo. Na vzpostavitev in izvedbo sistema upravljanja 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 upravljanja informacijske varnosti ohranja zaupnost, celovitost in razpoložljivost informacij z uporabo procesa za obvladovanje tveganj ter zainteresiranim strankam vzbuja zaupanje, da se tveganja ustrezno obvladujejo.

Pomembno je, da je sistem upravljanja 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 upravljanja informacijske varnosti skladno s potrebami organizacije.

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

Vrstni red predstavitve zahtev v tem mednarodnem standardu 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 upravljanja informacijske varnosti, pri čemer se sklicuje na skupino standardov za sisteme upravljanja 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 upravljanja

Ta mednarodni standard 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 upravljanja, ki so sprejeli dodatek SL.

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

Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

1 Področje uporabe

Ta mednarodni standard določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti v okviru organizacije. Zajema tudi zahteve za ocenjevanje in obravnavanje tveganj informacijske varnosti, ki so prilagojene potrebam organizacije. Zahteve, postavljene v tem mednarodnem standardu, so generične in so namenjene uporabi v vseh organizacijah ne glede na vrsto, velikost ali naravo. Izključevanje katere koli zahteve, določene v točkah 4 do 10, ni sprejemljivo, kadar organizacija zagotavlja skladnost s tem mednarodnim standardom.

2 Zveza s standardi

Ta dokument se v celoti ali v delih normativno sklicuje na naslednje dokumente, ki so nepogrešljivi pri njegovi uporabi. 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 upravljanja informacijske varnosti – Pregled in izrazoslovje

3 Izrazi in definicije

V tem dokumentu so uporabljeni izrazi in definicije, ki so podani v standardu ISO/IEC 27000.

4 Okvir organizacije

4.1 Razumevanje organizacije in njenega okvira

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 upravljanja informacijske varnosti.

OPOMBA: Določanje teh vprašanj se nanaša na opredelitev zunanjega in notranjega okvira organizacije iz točke 5.3 standarda ISO 31000:2009[5].

4.2 Razumevanje potreb in pričakovanj zainteresiranih strank

Organizacija mora določiti:

a) zainteresirane stranke, ki so pomembne za sistem upravljanja informacijske varnosti, in

b) zahteve teh zainteresiranih strank, ki so pomembne za informacijsko varnost.

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

4.3 Določitev obsega sistema upravljanja informacijske varnosti

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

Organizacija pri določanju tega obsega upošteva:

a) zunanja in notranja vprašanja iz točke 4.1,

b) zahteve iz točke 4.2 ter

c) povezave in odvisnosti med aktivnostmi, ki jih izvaja organizacija, in aktivnostmi, ki jih izvajajo druge organizacije.

Obseg mora biti na voljo v obliki dokumentiranih informacij.

4.4 Sistem upravljanja informacijske varnosti

Organizacija mora vzpostaviti, izvajati, vzdrževati in nenehno izboljševati sistem upravljanja informacijske varnosti v skladu z zahtevami tega mednarodnega standarda.

5 Voditeljstvo

5.1 Voditeljstvo in zavezanost

Najvišje vodstvo mora izkazovati sposobnost vodenja in zavezanost v zvezi s sistemom upravljanja informacijske varnosti z:

a) zagotavljanjem informacijske varnostne politike in postavljanjem ciljev informacijske varnosti, ki so združljivi s strateško usmeritvijo organizacije;

b) zagotavljanjem vključitve zahtev sistema upravljanja informacijske varnosti v procese organizacije;

c) zagotavljanjem razpoložljivosti virov, potrebnih za sistem upravljanja informacijske varnosti;

d) sporočanjem pomena uspešnega upravljanja informacijske varnosti in izpolnjevanjem zahtev sistema upravljanja informacijske varnosti;

e) zagotavljanjem, da sistem upravljanja informacijske varnosti dosega pričakovani(-e) rezultat(-e);

f) usmerjanjem in podpiranjem oseb za večjo uspešnost sistema upravljanja informacijske varnosti;

g) spodbujanjem nenehnega izboljševanja in

h) podpiranjem drugih pomembnih vodstvenih vlog za izkazovanje svojega voditeljstva v skladu s svojim področjem odgovornosti.

5.2 Politika

Najvišje vodstvo mora zagotavljati informacijsko varnostno politiko, ki:

a) ustreza namenu organizacije;

b) zajema cilje informacijske varnosti (glej točko 6.2) ali zagotavlja okvir za postavljanje ciljev informacijske varnosti;

c) zajema zavezanost k izpolnjevanju veljavnih zahtev v zvezi z informacijsko varnostjo in

d) zajema zavezanost k nenehnemu izboljševanju sistema upravljanja informacijske varnosti.

Informacijska varnostna politika mora biti:

e) na voljo v obliki dokumentiranih informacij;

f) sporočena znotraj organizacije in

g) po potrebi na voljo zainteresiranim strankam.

5.3 Organizacijske vloge, odgovornosti in pooblastila

Najvišje vodstvo mora zagotavljati, da so odgovornosti in pooblastila za vloge, pomembne za informacijsko varnost, določeni ter da so sporočeni vsem.

Najvišje vodstvo mora določiti odgovornosti in pooblastila za:

a) zagotavljanje, da je sistem upravljanja informacijske varnosti skladen z zahtevami tega mednarodnega standarda, in

b) poročanje najvišjemu vodstvu o delovanju sistema upravljanja informacijske varnosti.

OPOMBA: Najvišje vodstvo lahko določi tudi odgovornosti in pooblastila za poročanje o delovanju sistema upravljanja informacijske varnosti znotraj organizacije.

6 Načrtovanje

6.1 Ukrepi za obravnavanje tveganj in priložnosti

6.1.1 Splošno

Pri načrtovanju sistema upravljanja informacijske varnosti mora organizacija upoštevati vprašanja iz točke 4.1 in zahteve iz točke 4.2 ter določiti tveganja in priložnosti, ki jih je treba obravnavati, da:

a) zagotovi, da lahko sistem upravljanja informacijske varnosti doseže pričakovane rezultate;

b) prepreči ali omeji neželene učinke in

c) doseže nenehno izboljševanje.

Organizacija mora načrtovati:

d) ukrepe za obravnavanje teh tveganj in priložnosti ter

e) način, kako

1) vključiti ukrepe v procese svojega sistema upravljanja informacijske varnosti in jih izvajati ter

2) vrednotiti uspešnosti teh ukrepov.

6.1.2 Ocenjevanje tveganj informacijske varnosti

Organizacija mora določiti in uporabiti proces ocenjevanja tveganj informacijske varnosti, da:

a) vzpostavi in vzdržuje kriterije tveganj informacijske varnosti, ki zajemajo:

1) kriterije za sprejem tveganj in

2) kriterije za izvajanje ocenjevanja tveganj informacijske varnosti;

b) zagotavlja, da ponovljena ocenjevanja tveganj informacijske varnosti zagotavljajo dosledne, veljavne in primerljive rezultate;

c) prepozna tveganja informacijske varnosti:

1) uporabi proces ocenjevanja tveganj informacijske varnosti za prepoznavanje tveganj, povezanih z izgubo zaupnosti, celovitosti in razpoložljivosti za informacije v okviru sistema upravljanja informacijske varnosti, in

2) prepozna lastnike tveganj;

d) analizira tveganja informacijske varnosti:

1) oceni morebitne posledice, do katerih bi prišlo ob uresničitvi tveganj, prepoznanih v točki 6.1.2.c)(1),

2) oceni realno verjetnost pojava tveganj, prepoznanih v točki 6.1.2.c)(1), in

3) določi ravni tveganj;

e) ovrednoti tveganja informacijske varnosti:

1) primerja rezultate analize tveganj s kriteriji tveganj, postavljenimi v točki 6.1.2.a); in

2) prednostno razvrsti analizirana tveganja za obravnavanje tveganj.

Organizacija mora hraniti dokumentirane informacije o procesu ocenjevanja tveganj informacijske varnosti.

6.1.3 Obravnavanje tveganj informacijske varnosti

Organizacija mora določiti in uporabljati proces obravnavanja tveganj informacijske varnosti za:

a) izbiro ustreznih možnosti obravnavanja tveganj informacijske varnosti, pri čemer upošteva rezultate ocenjevanja tveganj;

b) določitev vseh kontrol, ki so potrebne za izvajanje izbranih možnosti obravnavanja tveganj informacijske varnosti;

OPOMBA: Organizacije lahko zasnujejo kontrole po potrebi ali jih opredelijo na podlagi katerega koli vira.

c) primerjavo kontrol iz gornje točke 6.1.3.b) s kontrolami iz dodatka A in preverjanje, da nobena potrebna kontrola ni bila izpuščena;

OPOMBA 1: Dodatek A vsebuje izčrpen seznam ciljev kontrol in kontrol. Uporabniki tega mednarodnega standarda naj upoštevajo dodatek A, da ne spregledajo nobene potrebne kontrole.

OPOMBA 2: Cilji kontrol so posredno vključeni v izbrane kontrole. Cilji kontrol in kontrole, navedeni v dodatku A, niso izčrpni in so morda potrebni dodatni cilji kontrol in kontrole.

d) pripravo izjave o uporabnosti, ki vsebuje potrebne kontrole (glej točko 6.1.3.b) in c)) ter utemeljitev za vključitev ne glede na to, ali so izvedene ali ne, ter utemeljitev za izključitev kontrol iz dodatka A;

e) pripravo načrta obravnavanja tveganj informacijske varnosti in

f) doseganje strinjanja lastnikov tveganj glede načrta obravnavanja tveganj informacijske varnosti ter sprejem preostalih tveganj informacijske varnosti.

Organizacija mora hraniti dokumentirane informacije o procesu obravnavanja tveganj informacijske varnosti.

OPOMBA: Proces ocenjevanja in obravnavanja tveganj informacijske varnosti v tem mednarodnem standardu je usklajen z načeli in splošnimi smernicami iz standarda ISO 31000[5].

6.2 Cilji informacijske varnosti in načrtovanje njihovega doseganja

Organizacija mora vzpostaviti cilje informacijske varnosti za ustrezne funkcije in ravni.

Cilji informacijske varnosti morajo:

a) biti skladni z informacijsko varnostno politiko;

b) biti merljivi (če je mogoče);

c) upoštevati veljavne zahteve informacijske varnosti ter rezultate ocenjevanja in obravnavanja tveganj;

d) biti sporočeni in

e) biti posodobljeni, če je to potrebno.

Organizacija mora hraniti dokumentirane informacije o ciljih informacijske varnosti.

Organizacija mora pri načrtovanju doseganja ciljev informacijske varnosti določiti:

f) kaj bo naredila,

g) kateri viri bodo potrebni,

h) kdo bo odgovoren,

i) kdaj bo delo končano in

j) kako bodo rezultati ovrednoteni.