SLOVENSKI STANDARD

SIST EN ISO/IEC 27002

maj 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)

Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

ICS 03.100.70; 35.030

Referenčna oznaka
SIST EN ISO/IEC 27002:2017 (sl)

Nadaljevanje na straneh II in od 1 do 88

NACIONALNI UVOD

Standard SIST EN ISO/IEC 27002 (sl, en), Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti (ISO/IEC 27002:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015), 2017, ima status slovenskega standarda in je enakovreden evropskemu standardu EN ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015), 2017.

NACIONALNI PREDGOVOR

Besedilo standarda EN ISO/IEC 27002:2017 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 27002:2017 je prevod angleškega besedila evropskega standarda EN ISO/IEC 27002:2017. 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 25. marca 2017 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda EN ISO/IEC 27002:2017

PREDHODNA IZDAJA

– SIST ISO/IEC 27002:2013, Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST EN ISO/IEC 27002:2017 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

– Ta nacionalni dokument je istoveten EN ISO/IEC 27002:2017 in je objavljen z dovoljenjem

CEN
Avenue Marnix 17
1050 Bruselj
Belgija

This national document is identical with EN ISO/IEC 27002:2017 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 27002

februar 2017

ICS: 03.100.70; 35.030

Slovenska izdaja

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

Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicher-heitsmaßnahmen (ISO/IEC 27002:2013 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

Vsebina **Stran**

Predgovor k evropskemu standardu

Besedilo standarda ISO/IEC 27002:2013, 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 27002:2017

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 27002:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015, je CEN odobril kot evropski standard EN ISO/IEC 27002:2017 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 iz 2. dela Direktiv ISO/IEC.

ISO/IEC 27002 je pripravil združeni tehnični odbor ISO/IEC JTC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

Opozoriti je treba na možnost, da so lahko nekateri elementi tega dokumenta predmet patentnih pravic. ISO ne prevzema odgovornosti za identifikacijo nekaterih ali vseh takih patentnih pravic.

Druga izdaja preklicuje in nadomešča prvo izdajo (ISO/IEC 27002:2005), ki je tehnično in strukturno revidirana.

0 Uvod

0.1 Ozadje in kontekst

Ta mednarodni standard je zasnovan, da bi ga organizacije uporabljale kot referenco pri izbiri kontrol znotraj procesa izvajanja sistema upravljanja informacijske varnosti (ISMS) na podlagi standarda ISO/IEC 27001[10] ali kot dokument z napotki za organizacije, ki izvajajo splošno sprejete kontrole informacijske varnosti. Ta standard je namenjen tudi za uporabo pri izdelavi smernic za upravljanje informacijske varnosti znotraj panog in organizacij, pri čemer upošteva posebne značilnosti njihovega okolja informacijskih varnostnih tveganj.

Organizacije vseh vrst in velikosti (vključno z javnim in zasebnim ter pridobitnim in nepridobitnim sektorjem) zbirajo, obdelujejo, shranjujejo in prenašajo informacije v mnogih oblikah, na primer elektronsko, fizično in ustno (npr. pogovori in predstavitve).

Vrednost informacij presega zapisane besede, številke in slike: znanje, koncepti, ideje in blagovne znamke so primeri neotipljivih oblik informacij. V medsebojno povezanem svetu so informacije ter povezani procesi, sistemi, omrežja in osebje, vključeno v njihovo delovanje, upravljanje in zaščito, dobrine, ki so kot druge pomembne poslovne dobrine dragocene za poslovanje organizacij in si kot take zaslužijo ali zahtevajo zaščito pred različnimi nevarnostmi.

Dobrine so predmet namernih in naključnih groženj, ranljivosti pa so sestavni del povezanih procesov, sistemov, omrežij in ljudi. Spremembe poslovnih procesov in sistemov ali druge zunanje spremembe (npr. spremembe zakonov in predpisov) lahko povzročijo nova informacijska varnostna tveganja. Zaradi velikega števila načinov, na katere lahko grožnje izkoristijo ranljivosti in škodijo organizacijam, so informacijska varnostna tveganja vedno prisotna. Z zaščito organizacije pred grožnjami in ranljivostmi uspešna informacijska varnost zmanjša ta tveganja in nato njihove učinke na dobrine organizacije.

Informacijska varnost se doseže z izvajanjem ustreznih nizov kontrol, vključno s politikami, procesi, postopki, organizacijskimi strukturami ter funkcijami programske in strojne opreme. Te kontrole je treba vzpostaviti, izvajati, spremljati, pregledovati in izboljševati, kadar je to potrebno, da se zagotovi, da so izpolnjeni posebni varnostni in poslovni cilji organizacije. Sistem upravljanja informacijske varnosti, kot je naveden v standardu SO/IEC 27001[10], omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije, da lahko izvaja celovit niz kontrol informacijske varnosti v okviru koherentnega sistema upravljanja.

Mnogi informacijski sistemi niso bili zasnovani kot varni sistemi v smislu standarda ISO/IEC 27001[10] in tega standarda. Varovanje, ki ga je mogoče doseči s tehničnimi sredstvi, je omejeno ter naj bo podprto z ustreznim upravljanjem in postopki. Prepoznavanje, katere kontrole naj bodo nameščene, zahteva skrbno načrtovanje in osredotočenost na podrobnosti. Za uspešen sistem upravljanja informacijske varnosti je potrebno sodelovanje vseh zaposlenih v organizaciji. Prav tako je lahko potrebna udeležba delničarjev, dobaviteljev ali drugih zunanjih strank. Potrebni pa so lahko tudi strokovni nasveti zunanjih strank.

V bolj splošnem pomenu uspešna informacijska varnost zagotavlja vodstvu in drugim deležnikom, da so dobrine organizacije primerno varne in zaščitene pred škodo, zato omogoča boljše poslovanje.

0.2 Zahteve informacijske varnosti

Bistveno je, da organizacija prepozna svoje varnostne zahteve. Glavni viri varnostnih zahtev so trije:

a) ocenjevanje tveganj organizacije ob upoštevanju celovite poslovne strategije in ciljev organizacije. Z oceno tveganj se prepoznajo grožnje dobrinam, ovrednotita se ranljivost in verjetnost pojava ter oceni se potencialni vpliv;

b) pravne, zakonske, regulativne in pogodbene zahteve, ki jih morajo izpolniti organizacija, njeni poslovni partnerji, pogodbeniki in ponudniki storitev, ter njihovo družbeno-kulturno okolje;

c) niz načel, ciljev in poslovnih zahtev za upravljanje, obdelavo, shranjevanje, prenos in shranjevanje informacij, ki ga je organizacija razvila za podporo svojemu delovanju.

Viri, ki se uporabljajo za izvajanje kontrol, morajo biti zaščiteni pred poslovno škodo, do katere utegne priti zaradi varnostnih tveganj zaradi odsotnosti takih kontrol. Rezultati ocenjevanja tveganj bodo pomagali voditi in določiti ustrezne ukrepe vodstva in prednostne naloge za upravljanje informacijskih varnostnih tveganj ter za izvajanje kontrol, izbranih za varovanje pred temi tveganji.

Standard ISO/IEC 27005[11] podaja navodila za upravljanje informacijskih varnostnih tveganj, vključno z napotkom za ocenjevanje, obravnavanje in sprejetje tveganj, obveščanje o tveganjih ter za spremljanje in pregled tveganj.

0.3 Izbiranje kontrol

Kontrole se lahko izberejo iz tega standarda ali drugih nizov kontrol ali pa se lahko zasnujejo nove kontrole za izpolnitev ustreznih posebnih potreb.

Izbor kontrol je odvisen od organizacijskih odločitev, ki temeljijo na kriterijih za sprejetje tveganj, možnostih obravnavanja tveganj ter na splošnem pristopu k upravljanju tveganj, ki ga uporablja organizacija, ter naj ustreza vsem ustreznim nacionalnim in mednarodnim zakonodajam in predpisom. Izbira kontrol je odvisna tudi od načina, kako kontrole vzajemno delujejo, kar omogoča globoko zaščito.

Nekatere kontrole v tem standardu je mogoče obravnavati kot vodilna načela za upravljanje informacijske varnosti in ustrezajo večini organizacij. Te kontrole so podrobneje razložene spodaj skupaj z napotki za izvajanje. Več informacij o izbiranju kontrol in drugih možnostih obravnavanja tveganj je mogoče najti v standardu ISO/IEC 27005. [11]

0.4 Razvijanje lastnih smernic

Ta mednarodni standard je mogoče upoštevati kot izhodišče za razvoj posebnih smernic organizacije. Vse kontrole in smernice iz teh pravil obnašanja morda niso primerne. Poleg tega so lahko potrebne dodatne kontrole in smernice, ki niso vključene v ta standard. Ko bodo razviti dokumenti z dodatnimi kontrolami ali smernicami, bo morda koristno vključiti sklice na točke v tem standardu, kjer je to primerno, kar bo olajšalo preverjanje skladnosti presojevalcem in poslovnim partnerjem.

0.5 Razmisleki o življenjskem ciklu

Informacije imajo naravni življenjski cikel: od ustvarjanja in nastanka prek shranjevanja, obdelave in prenosa do morebitnega uničenja ali propada. Vrednost dobrin in tveganj zanje se lahko med življenjskim ciklom spreminjajo (npr. nepooblaščeno razkritje ali kraja finančnih računov podjetja je manj pomembna, potem ko so bili že uradno objavljeni), vendar informacijska varnost ostaja relativno pomembna v vseh obdobjih.

Informacijski sistemi imajo življenjske cikle, znotraj katerih so ustvarjeni, določeni, načrtovani, razviti, testirani, uvedeni, uporabljeni, vzdrževani in morebiti umaknjeni oziroma zavrženi. Informacijska varnost bi morala biti upoštevana v vsakem obdobju. Razvoj novih in spremembe obstoječih sistemov organizacijam omogočajo, da posodobijo in izboljšajo varnostne kontrole, pri tem pa upoštevajo dejanske incidente ter trenutna in predvidena informacijska varnostna tveganja.

0.6 Sorodni standardi

Čeprav ta standard podaja smernice za širok razpon kontrol informacijske varnosti, ki se navadno uporabljajo v številnih različnih organizacijah, drugi standardi skupine ISO/IEC 27000 podajajo dodatne zahteve ali nasvete o drugih vidikih celotnega procesa upravljanja informacijske varnosti.

Splošni uvod v sisteme upravljanja informacijske varnosti in skupino standardov je podan v standardu ISO/IEC 27000. Standard ISO/IEC 27000 vsebuje glosar, v katerem je uradno definirana večina izrazov, ki se uporabljajo v skupini standardov ISO/IEC 27000. Ta standard opisuje tudi področje uporabe in cilje vsakega standarda v skupini.

Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti

1 Področje uporabe

Ta mednarodni standard podaja smernice za standarde informacijske varnosti organizacij in načine uporabe upravljanja informacijske varnosti, kar vključuje izbiro, izvajanje in upravljanje kontrol, pri čemer upošteva informacijska varnostna tveganja okolja(-ij) organizacije.

Ta mednarodni standard je zasnovan, da ga uporabijo organizacije, ki želijo:

a) izbrati kontrole znotraj procesa izvajanja sistema upravljanja informacijske varnosti na podlagi ISO/IEC 27001,[10]

b) izvajati splošno sprejete kontrole informacijske varnosti,

c) razvijati lastne smernice za upravljanje informacijske varnosti.

2 Zveze s standardi

Pri uporabi tega standarda so, delno ali v celoti, nujno potrebni spodaj navedeni referenčni dokumenti. Pri datiranih sklicevanjih se uporablja le navedena izdaja. Pri nedatiranih sklicevanjih se uporablja zadnja izdaja publikacije (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, podani v ISO/IEC 27000.

4 Struktura tega standarda

Ta standard vsebuje 14 točk o varnostnih kontrolah, ki skupaj tvorijo 35 glavnih varnostnih kategorij in 114 kontrol.

4.1 Točke

Vsaka točka, ki definira varnostne kontrole, vsebuje eno ali več glavnih varnostnih kategorij.

Vrstni red točk v tem standardu ne nakazuje njihove pomembnosti. Varnostne kontrole iz vseh ali katere koli točke so lahko pomembne, odvisno od okoliščin, zato naj vsaka organizacija, ki uporablja ta standard, določi njihovo pomembnost in uporabo v posameznih poslovnih procesih. Prav tako seznami v tem standardu niso zapisani v prednostnem vrstnem redu.

4.2 Kategorije kontrol

Vsaka glavna kategorija varnostnih kontrol vsebuje:

a) cilj kontrole, ki navaja, kaj je treba doseči,

b) eno ali več kontrol, ki jih je mogoče uporabiti za doseganje cilja kontrole.

Opisi kontrol so strukturirani na naslednji način:

Kontrola
Določa specifične kontrolne izjave za izpolnitev cilja kontrole.

Napotki za izvajanje
Zagotavljajo podrobnejše informacije v podporo izvedbi kontrole in doseganju njenega cilja. Napotki morda niso popolnoma primerni ali zadostni v vseh situacijah in morda ne izpolnijo posebnih zahtev kontrole organizacije.

Druge informacije
Zagotovijo nadaljnje informacije, ki jih je morda treba upoštevati, na primer pravne vidike in sklicevanje na druge standarde. Če druge informacije niso podane, tega dela besedila ni.

5 Informacijske varnostne politike

5.1 Usmeritev vodstva za informacijsko varnost

Cilj: Zagotoviti usmeritve vodstva in njegovo podporo informacijski varnosti v skladu s poslovnimi zahtevami ter ustreznimi zakoni in predpisi.

5.1.1 Politike za informacijsko varnost

Kontrola
Opredeli naj se sklop politik za informacijsko varnost, ki jih odobri vodstvo, ter se objavi in sporoči zaposlenim in ustreznim zunanjim strankam.

Napotki za izvajanje
Organizacije naj na najvišji ravni opredelijo "informacijsko varnostno politiko", ki jo odobri vodstvo in ki določi pristop organizacije k upravljanju njenih ciljev informacijske varnosti.

Informacijske varnostne politike naj obravnavajo zahteve, ki jih ustvarijo:

a) poslovna strategija,

b) predpisi, zakonodaja in pogodbe,

c) trenutno in predvideno okolje groženj informacijski varnosti.

Informacijska varnostna politika naj vsebuje izjave o:

a) definiciji informacijske varnosti ter ciljih in načelih za vodenje vseh aktivnosti, povezanih z informacijsko varnostjo,

b) dodeljevanju splošnih in posebnih odgovornosti za upravljanje informacijske varnosti določenim vlogam,

c) procesih za ravnanje ob odstopanjih in izjemah.

Na nižji ravni naj informacijsko varnostno politiko podpirajo temi ustrezne politike, ki podelijo nadaljnja pooblastila za izvajanje kontrol informacijske varnosti in so navadno strukturirane za obravnavo potreb določenih ciljnih skupin v organizaciji ali da obravnavajo določene teme.

Primeri takih tem politike so:

a) nadzor dostopa (glej točko 9);

b) razvrstitev (in obravnavanje) informacij (glej 8.2);

c) fizična in okoljska varnost (glej točko 11);

d) teme, usmerjene na končnega uporabnika, kot so:

   1) sprejemljiva uporaba dobrin (glej 8.1.3),

   2) čista miza in prazen zaslon (glej 11.2.9),

   3) prenos informacij (glej 13.2.1),

   4) mobilne naprave in delo na daljavo (glej 6.2),

   5) omejitve namestitve in uporabe programske opreme (glej 12.6.2);

e) varnostno kopiranje (glej 12.3);

f) prenos informacij (glej 13.2);

g) zaščita pred zlonamerno programsko opremo (glej 12.2);

h) upravljanje tehničnih ranljivosti (glej 12.6.1);

i) kriptografske kontrole (glej točko 10);

j) komunikacijska varnost (glej točko 13);

k) zasebnost in zaščita osebno določljivih podatkov (glej 18.1.4);

l) odnosi z dobavitelji (glej točko 15).

S temi politikami naj bodo seznanjeni zaposleni in ustrezne zunanje stranke na način, ki bo predvidenemu bralcu ustrezen, dostopen in razumljiv, npr. v kontekstu "spoznavanja informacijske varnosti, izobraževanja in usposabljanja" (glej 7.2.2).

Druge informacije
Potreba po notranjih politikah za informacijsko varnost se v različnih delih organizacije razlikuje. Notranje politike so posebej uporabne v večjih in bolj zapletenih organizacijah, kjer so tisti, ki določajo in potrjujejo pričakovane ravni nadzora, ločeni od tistih, ki nadzor izvajajo, ali v primerih, ko politika velja za številne različne ljudi ali funkcije v organizaciji. Informacijske varnostne politike je mogoče izdati v enem dokumentu "informacijske varnostne politike" ali v naboru posameznih, a med seboj povezanih dokumentov.

Če se katera koli od informacijskih varnostnih politik razširja zunaj organizacije, naj se pazi, da se ne razkrijejo zaupne informacije.

Nekatere organizacije uporabljajo druge izraze za te dokumente, kot so "standardi", "direktive" ali "pravila".

5.1.2 Pregled politik za informacijsko varnost

Kontrola
Politike za informacijsko varnost naj se pregledujejo v načrtovanih intervalih ali če se pojavijo pomembne spremembe, da se zagotovijo njihova nenehna ustreznost, zadostnost in uspešnost.

Napotki za izvajanje
Vsaka politika naj ima lastnika, ki mu je vodstvo določilo odgovornost za razvoj, pregled in vrednotenje politik. Pregled naj vključuje ocenjevanje možnosti za izboljšanje politik organizacije in pristop k upravljanju informacijske varnosti kot odgovor na spremembe v organizacijskem okolju, poslovnih okoliščinah, pravnih pogojih ali tehničnem okolju.

Pregled politik za informacijsko varnost naj upošteva rezultate vodstvenih pregledov.

Za revidirane politike naj se pridobi odobritev vodstva.

6 Organiziranje informacijske varnosti

6.1 Notranja organizacija

Cilj: Vzpostaviti okvir upravljanja za začetek in kontrolo izvajanja ter delovanja informacijske varnosti v organizaciji.

6.1.1 Vloge in odgovornosti na področju informacijske varnosti

Kontrola
Določijo in dodelijo naj se vse odgovornosti na področju informacijske varnosti.