
Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti / Opomba: Združuje ISO/IEC 17799 (2005-06) (preštevilčen v ISO/IEC 27002) in ISO/IEC 17799 Tehnični popravek 1 (2007-07)

Information technology – Security techniques – Code of practice for information security management / Note: Combines ISO/IEC 17799 (2005-06) (renumbered to ISO/IEC 27002) and ISO/IEC 17799 Technical Corrigendum 1 (2007-07)

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

NACIONALNI UVOD

Standard SIST ISO/IEC 27002 (sl), Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti, 2008, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27002 (en), Information technology – Security techniques – Code of practice for information security management, prva izdaja, 2005-06-15.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27002:2005 je pripravil pododbor združenega tehničnega odbora Mednarodne organizacije za standardizacijo in Mednarodne elektrotehniške komisije ISO/IEC JTC 1/SC 27 Varnostne tehnike v informacijski tehnologiji.

Slovenski standard SIST ISO/IEC 27002:2008 je prevod mednarodnega standarda ISO/IEC 27002:2005. Slovenski standard SIST ISO/IEC 27002:2008 je pripravil tehnični odbor SIST/TC ITC Informacijska tehnologija. V primeru spora glede besedila slovenskega prevoda je odločilen izvorni mednarodni standard v angleškem jeziku.

Odločitev za izdajo tega standarda je dne 27. marca 2008 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDARDA

- privzem standarda ISO/IEC 27002:2005

OPOMBE

iTeh STANDARD PREVIEW

- Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST ISO/IEC 27002:2008 to pomeni "slovenski standard".
- Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.
<https://standards.iteh.ai/catalog/standards/sist/980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>
- Definicije pojmov so povzete po naslednjih mednarodnih standardih:
 - ISO/IEC 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
 - ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management
 - ISO/IEC Guide 2, Standardization and related activities – General vocabulary
 - ISO/IEC Guide 73, Risk management – Vocabulary
- V besedilu SIST ISO/IEC 27002 so v točkah 2.1, 2.3, 2.6, 2.7, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 4.1, 5.1.1, 6.1.1, 6.1.8, 7.1.1, 10.6.1, 12.1.1, 12.3.1, 12.3.2, 12.4.3, 12.5.4, 13.1.1 in 15.1.3 navedeni mednarodni standardi ISO/IEC 13335-1, ISO/IEC 13335-3, ISO/IEC TR 18044, ISO 19011, ISO/IEC 18028, ISO/IEC 11770, ISO/IEC 9796, ISO/IEC 14888, ISO 10007, ISO/IEC 12207, ISO/IEC 15408, ISO 15489-1, ISO/IEC Guide 2, ISO/IEC Guide 73 in IEEE P1363. Pri tem je vedno mišljena njihova zadnja izdaja.
- Standard ISO/IEC 17799 je bil leta 2007 preštevilčen v ISO/IEC 27002.

VSEBINA	Stran
Predgovor k standardu ISO/IEC 27002:2005.....	8
Predgovor k standardu ISO/IEC 17799:2005.....	9
0 Uvod	10
0.1 Kaj je informacijska varnost.....	10
0.2 Zakaj je informacijska varnost potrebna.....	10
0.3 Kako vzpostaviti varnostne zahteve	10
0.4 Ocenjevanje varnostnih tveganj	11
0.5 Izbiranje kontrol	11
0.6 Izhodišče informacijske varnosti	11
0.7 Ključni dejavniki uspeha	12
0.8 Razvijanje lastnih smernic.....	12
1 Področje uporabe	13
2 Izrazi in definicije	13
3 Struktura tega standarda.....	15
3.1 Točke.....	15
3.2 Glavne varnostne kategorije.....	15
4 Ocenjevanje in obravnavanje tveganja	16
4.1 Ocenjevanje varnostnih tveganj	16
4.2 Obravnavanje varnostnih tveganj	16
5 Varnostna politika	17
5.1 Informacijska varnostna politika	17
5.1.1 Dokument o informacijski varnostni politiki	17
5.1.2 Pregled informacijske varnostne politike.....	18
6 Organiziranje informacijske varnosti	19
6.1 Notranja organizacija.....	19
6.1.1 Zavezanost vodstva k informacijski varnosti	19
6.1.2 Usklajevanje informacijske varnosti	20
6.1.3 Dodelitev odgovornosti na področju informacijske varnosti	20
6.1.4 Proces odobritve naprav za obdelavo informacij	21
6.1.5 Dogovori o zaupnosti.....	21
6.1.6 Stiki s pristojnimi organi.....	22
6.1.7 Stik s specifičnimi interesnimi skupinami	22
6.1.8 Neodvisni pregled informacijske varnosti.....	23
6.2 Zunanje stranke	23
6.2.1 Prepoznavanje tveganj, povezanih z zunanjimi strankami	23
6.2.2 Obravnavanje varnosti pri poslovanju s strankami	25
6.2.3 Obravnavanje varnosti v dogovorih s tretjimi strankami	26
7 Upravljanje dobrin.....	28
7.1 Odgovornost za dobrine	28
7.1.1 Popis dobrin.....	28

7.1.2 Lastništvo nad dobrinami	29
7.1.3 Sprejemljiva uporaba dobrin.....	29
7.2 Razvrstitev informacij	30
7.2.1 Smernice za razvrščanje	30
7.2.2 Označevanje informacij in ravnanje z njimi	30
8 Varnost človeških virov.....	31
8.1 Pred zaposlovanjem.....	31
8.1.1 Vloge in odgovornosti.....	31
8.1.2 Preverjanje	32
8.1.3 Določila in pogoji za zaposlitev	32
8.2 Med zaposlitvijo	33
8.2.1 Odgovornosti vodstva.....	33
8.2.2 Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti	34
8.2.3 Disciplinski proces.....	34
8.3 Prekinitev ali sprememba zaposlitve.....	35
8.3.1 Odgovornosti ob prenehanju zaposlitve.....	35
8.3.2 Vračilo dobrin.....	36
8.3.3 Preklic pravic dostopa	36
9 Fizična in okoljska varnost	37
9.1 Varovana območja	37
9.1.1 Varovanje fizičnih meja območja.....	37
9.1.2 Kontrole fizičnega vstopa	38
9.1.3 Varovanje pisarn, sob in naprav.....	38
9.1.4 Zaščita pred zunanji in okoljskimi grozljami.....	38
9.1.5 Delo na varovanih območjih.....	39
9.1.6 Javni dostop, dostavne in nakladalne površine	39
9.2 Varnost opreme	40
9.2.1 Namestitev in zaščita opreme	40
9.2.2 Podporna oskrba	40
9.2.3 Varnost ožičenja	41
9.2.4 Vzdrževanje opreme	42
9.2.5 Varnost opreme zunaj prostorov organizacije.....	42
9.2.6 Varna odstranitev ali ponovna uporaba opreme	43
9.2.7 Odstranitev premoženja	43
10 Upravljanje komunikacij in obratovanja.....	43
10.1 Operativni postopki in odgovornosti	43
10.1.1 Dokumentirani postopki delovanja	44
10.1.2 Upravljanje sprememb	44
10.1.3 Razmejitev dolžnosti	45
10.1.4 Ločevanje razvojnih, testnih in obratovalnih naprav	45
10.2 Upravljanje storitev tretjih strank	46
10.2.1 Izvedba storitev	46

10.2.2 Spremljanje in pregledovanje storitev tretjih strank	46
10.2.3 Upravljanje sprememb storitev tretjih strank	47
10.3 Načrtovanje in prevzem sistema	48
10.3.1 Upravljanje zmogljivosti	48
10.3.2 Prevzem sistema	48
10.4 Zaščita pred zlonamerno in mobilno kodo	49
10.4.1 Kontrole za zaščito pred zlonamerno kodo	49
10.4.2 Kontrole nad mobilno kodo	50
10.5 Varnostno kopiranje	51
10.5.1 Varnostno kopiranje informacij	51
10.6 Upravljanje varovanja omrežij	52
10.6.1 Omrežne kontrole	52
10.6.2 Varovanje omrežnih storitev	52
10.7 Ravnanje z nosilci podatkov/informacij	53
10.7.1 Upravljanje izmenljivih nosilcev podatkov/informacij	53
10.7.2 Odstranjevanje nosilcev podatkov/informacij	54
10.7.3 Postopki ravnanja z informacijami	54
10.7.4 Varovanje systemske dokumentacije	55
10.8 Izmenjava informacij	55
10.8.1 Politike in postopki izmenjave informacij	55
10.8.2 Dogovori o izmenjavi	57
10.8.3 Fizični nosilci podatkov/informacij med prenašanjem	57
10.8.4 Elektronsko sporočanje	58
10.8.5 Poslovni informacijski sistemi	58
10.9 Storitve elektronskega poslovanja	59
10.9.1 Elektronsko poslovanje	59
10.9.2 Sprotno transakcije	60
10.9.3 Javno dostopne informacije	61
10.10 Spremljanje	62
10.10.1 Beleženje dogodkov za zagotavljanje revizijske sledi	62
10.10.2 Spremljanje uporabe sistema	62
10.10.3 Zaščita zabeleženih informacij	64
10.10.4 Beleženje aktivnosti administratorjev in operaterjev	64
10.10.5 Beleženje okvar	64
10.10.6 Uskladitev ur	65
11 Nadzor dostopa	65
11.1 Poslovne zahteve za nadzor dostopa	65
11.1.1 Politika nadzora dostopa	65
11.2 Upravljanje uporabniškega dostopa	67
11.2.1 Registracija uporabnika	67
11.2.2 Upravljanje posebnih dostopnih pravic	68
11.2.3 Upravljanje uporabniških gesel	68

11.2.4 Pregled uporabniških pravic dostopa	69
11.3 Odgovornosti uporabnikov	69
11.3.1 Uporaba gesel	69
11.3.2 Nenadzorovana uporabniška oprema	70
11.3.3 Politiki čiste mize in praznega zaslona	70
11.4 Nadzor dostopa do omrežja	71
11.4.1 Politika uporabe omrežnih storitev	71
11.4.2 Preverjanje verodostojnosti uporabnikov oddaljenih povezav	72
11.4.3 Istovetnost opreme v omrežjih	72
11.4.4 Zaščita vrat za oddaljeno diagnosticiranje in konfiguriranje	73
11.4.5 Ločevanje v omrežjih	73
11.4.6 Nadzor omrežne povezave	74
11.4.7 Nadzor usmerjanja v omrežjih	74
11.5 Nadzor dostopa do operacijskih sistemov	75
11.5.1 Varni postopki prijave	75
11.5.2 Preverjanje istovetnosti in verodostojnosti uporabnika	76
11.5.3 Sistem upravljanja gesel	76
11.5.4 Uporaba sistemskih pripomočkov	77
11.5.5 Prekinitev seje	78
11.5.6 Omejitev časa povezave	78
11.6 Nadzor dostopa do aplikacij in informacij	78
11.6.1 Omejitev dostopa do informacij	79
11.6.2 Izolacija občutljivih sistemov	79
11.7 Mobilno računalništvo in delo na daljavo	79
11.7.1 Mobilno računalništvo in komunikacije	80
11.7.2 Delo na daljavo	81
12 Pridobivanje, razvoj in vzdrževanje informacijskih sistemov	82
12.1 Varnostne zahteve informacijskih sistemov	82
12.1.1 Analiza in specifikacije varnostnih zahtev	82
12.2 Pravilna obdelava v aplikacijah	83
12.2.1 Potrjevanje vhodnih podatkov	83
12.2.2 Nadzor notranje obdelave	83
12.2.3 Celovitost sporočil	84
12.2.4 Potrjevanje izhodnih podatkov	85
12.3 Kriptografske kontrole	85
12.3.1 Politika uporabe kriptografskih kontrol	85
12.3.2 Upravljanje ključev	86
12.4 Varnost sistemskih datotek	87
12.4.1 Nadzor operativne programske opreme	87
12.4.2 Zaščita sistemskih testnih podatkov	88
12.4.3 Nadzor dostopa do programske izvorne kode	89
12.5 Varnost v procesih razvoja in podpore	90

12.5.1 Postopki nadzora sprememb	90
12.5.2 Tehnični pregled aplikacij po spremembah operacijskih sistemov	91
12.5.3 Omejitve pri spremembah programskih paketov	91
12.5.4 Uhajanje informacij.....	91
12.5.5 Zunanje izvajanje razvoja programske opreme	92
12.6 Tehnično upravljanje ranljivosti	92
12.6.1 Nadzor tehničnih ranljivosti	92
13 Upravljanje informacijskih varnostnih incidentov	94
13.1 Poročanje o informacijskih varnostnih dogodkih in pomanjkljivostih	94
13.1.1 Poročanje o informacijskih varnostnih dogodkih.....	94
13.1.2 Poročanje o varnostnih pomanjkljivostih	95
13.2 Upravljanje informacijskih varnostnih incidentov in izboljšave.....	95
13.2.1 Odgovornosti in postopki.....	96
13.2.2 Učenje iz informacijskih varnostnih incidentov.....	97
13.2.3 Zbiranje dokazov	97
14 Upravljanje neprekinjenega poslovanja	98
14.1 Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja	98
14.1.1 Vključevanje informacijske varnosti v proces upravljanja neprekinjenega poslovanja.....	98
14.1.2 Neprekinjeno poslovanje in ocenjevanje tveganja	99
14.1.3 Razvoj in izvajanje načrtov neprekinjenega poslovanja z vključevanjem informacijske varnosti	99
14.1.4 Okvir načrtovanja neprekinjenega poslovanja	100
14.1.5 Testiranje, vzdrževanje in ponovno ocenjevanje načrtov neprekinjenega poslovanja	101
15 Skladnost	102
15.1 Skladnost z zakonodajo	102
15.1.1 Prepoznavanje veljavne zakonodaje.....	102
15.1.2 Pravice intelektualne lastnine.....	102
15.1.3 Zaščita organizacijskih zapisov	103
15.1.4 Zaščita podatkov in zasebnost osebnih podatkov	104
15.1.5 Preprečevanje zlorabe naprav za obdelavo informacij	104
15.1.6 Uporaba kriptografskih kontrol	105
15.2 Skladnost z varnostnimi politikami in standardi ter tehnična skladnost	106
15.2.1 Skladnost z varnostnimi politikami in standardi	106
15.2.2 Tehnično preverjanje skladnosti.....	106
15.3 Upoštevanje presoj informacijskih sistemov	107
15.3.1 Kontrole presoje informacijskih sistemov	107
15.3.2 Zaščita orodij za presojo informacijskih sistemov	107
Literatura	109
Indeks	110

Predgovor k standardu ISO/IEC 27002:2005

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

Prva izdaja tega standarda ISO/IEC 27002 združuje ISO/IEC 17799:2005 in ISO/IEC 17799:2005/Cor.1:2007. Njena tehnična vsebina je istovetna vsebini ISO/IEC 17799:2005. Popravek ISO/IEC 17799:2005/Cor.1:2007 spreminja referenčno številko standarda iz 17799 v 27002. ISO/IEC 17799:2005 in ISO/IEC 17799:2005/Cor.1:2007 sta začasno zadržana do objave druge izdaje ISO/IEC 27002.

[SIST ISO/IEC 27002:2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

Predgovor k standardu ISO/IEC 17799:2005

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 pripravljani 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 17799 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija*, pododbor SC 27 *Varnostne tehnike IT*.

Ta druga izdaja razveljavlja in nadomešča prvo izdajo (ISO/IEC 17799:2000), ki je bila tehnično spremenjena.

Skupina mednarodnih standardov o sistemu upravljanja informacijske varnosti (ISMS) se razvija v okviru ISO/IEC JTC 1/SC 27. Skupina vključuje mednarodne standarde o zahtevah za sistem upravljanja informacijske varnosti, obvladovanje tveganja, metrike in merjenja ter napotke za izvajanje. Ta družina bo sprejela sistem številčenja z nizom številčk 27000 in zaporedno naprej.

Od leta 2007 se predlaga vključitev nove izdaje ISO/IEC 17799 v to novo shemo številčenja kot ISO/IEC 27002.

0 Uvod

0.1 Kaj je informacijska varnost

Informacija je dobrina, ki je tako kot druge pomembne poslovne dobrine bistvenega pomena za poslovanje organizacije in jo je zato treba ustrezno zaščititi. To je še posebej pomembno v sedanjem, vse bolj povezanem poslovnem okolju. Kot rezultat tega povečanja medsebojne povezanosti so informacije zdaj vse bolj izpostavljene različnim grožnjam in ranljivostim (glej tudi Smernice OECD za varnost informacijskih sistemov in omrežij).

Informacija lahko obstaja v različnih oblikah. Lahko je natisnjena ali napisana na papirju, shranjena v elektronski obliki, prenesena po pošti ali z uporabo elektronskih sredstev, prikazana na filmu ali izgovorjena v pogovoru. Ne glede na obliko informacije ali sredstva, s katerim je v skupni rabi, mora vedno biti ustrezno zaščitena.

Informacijska varnost je zaščita informacij pred različnimi grožnjami, da bi zagotovili neprekinjeno poslovanje, zmanjšali poslovno tveganje ter čim bolj povečali donosnost naložb in poslovnih priložnosti.

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. To je treba storiti v povezavi z drugimi procesi upravljanja poslovanja.

0.2 Zakaj je informacijska varnost potrebna

Informacije in podporni procesi, sistemi in omrežja so pomembne poslovne dobrine. Oprelitev, doseganje, vzdrževanje in izboljševanje informacijske varnosti so lahko bistvenega pomena za ohranjanje konkurenčne prednosti, denarnega toka, dobičkonosnosti, skladnosti z zakonodajo in poslovno podobo. <https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

Organizacije ter njihovi informacijski sistemi in omrežja se soočajo z varnostnimi grožnjami iz širokega spektra virov, vključno z računalniško podprtimi prevarami, vohunstvom, sabotажami, vandalizmom, požari ali poplavami. Vzroki za poškodbe, kot so zlonamerne kode, računalniško vlamljanje in napadi za zavrnitev storitve, so postali pogostejši, ambicioznejši ter vse bolj prefinjeni.

Informacijska varnost je pomembna tako za javni kot za zasebni poslovni sektor ter za varovanje kritične infrastrukture. V obeh sektorjih bo informacijska varnost delovala kot dejavnik, ki omogoča na primer doseči e-upravo ali e-poslovanje, ter preprečuje ali zmanjšuje tveganja. Povezovanje javnih in zasebnih omrežij ter skupna raba informacijskih virov povečujeta težave pri doseganju nadzora dostopa. Trend porazdeljenega računalništva je tudi oslabil uspešnost osrednje, specializirane kontrole.

Mnogi informacijski sistemi niso bili zasnovani kot varni. Varovanje, ki ga je mogoče doseči s tehničnimi sredstvi, je omejeno ter naj bi bilo podprto z ustreznim upravljanjem in postopki. Prepoznavanje ustrezne kontrole naj se skrbno načrtuje in osredotoča na podrobnosti. Upravljanje informacijske varnosti najmanj zahteva sodelovanje vseh zaposlenih v organizaciji. Prav tako lahko zahteva udeležbo delničarjev, dobaviteljev, tretjih oseb, odjemalcev ali drugih zunanjih strank. Potrebni so lahko tudi strokovni nasveti zunanjih organizacij.

0.3 Kako vzpostaviti varnostne zahteve

Bistveno je, da organizacija prepozna svoje varnostne zahteve. Obstajajo trije glavni viri varnostnih zahtev.

1. En vir je izpeljan iz ocenjevanja tveganj organizacije ob upoštevanju celovite poslovne organizacijske strategije in ciljev. Z oceno tveganja se prepoznajo grožnje dobrinam, ovrednotijo se ranljivost in verjetnost pojava ter ocenijo se potencialni vplivi.
2. Drug vir so pravne, zakonske in regulativne zahteve, ki jih morajo izpolniti organizacija, njeni poslovni partnerji, izvajalci in ponudniki storitev, ter njihovo družbeno-kulturno okolje.
3. Dodatni vir je še poseben niz načel, ciljev in poslovnih zahtev za obdelave informacij, ki jih je organizacija razvila v podporo svojega poslovanja.

0.4 Ocenjevanje varnostnih tveganj

Varnostne zahteve se prepoznajo z metodičnim ocenjevanjem varnostnih tveganj. Izdatke za kontrole je treba uravnotežiti glede na poslovno škodo, ki navadno izhaja iz napak pri varovanju.

Rezultati ocenjevanja tveganja bodo pomagali voditi in določiti ustrezne ukrepe vodstva in prednostne naloge za obvladovanje informacijskih varnostnih tveganj ter za izvajanje kontrol, izbranih za varovanje pred temi tveganji.

Ocenjevanje tveganja naj se redno ponavlja in obravnava vse spremembe, ki lahko vplivajo na rezultate ocenjevanja tveganja.

Več informacij o ocenjevanju varnostnih tveganj je mogoče najti v točki 4.1 Ocenjevanje varnostnih tveganj.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

0.5 Izbiranje kontrol

SIST ISO/IEC 27002:2008

Ko so varnostne zahteve in tveganja prepoznani in so sprejete odločitve za obravnavanje tveganj, naj se izberejo in izvajajo ustrezne kontrole, da se tveganja zmanjšajo na sprejemljivo raven. Kontrole je mogoče izbrati iz tega standarda ali drugih nizov ukrepov, lahko pa se zasnujejo tudi nove kontrole za zadovoljitev posebnih potreb. Izbor varnostnih ukrepov je odvisen od organizacijskih odločitev, ki temeljijo na kriterijih za sprejem tveganja, možnostih obravnavanja tveganja ter na splošnem pristopu k upravljanju tveganja, ki ga uporablja organizacija, ter naj ustreza vsem ustreznim nacionalnim in mednarodnim zakonodajam in predpisom.

Nekatere kontrole v tem standardu je mogoče obravnavati kot vodilna načela za upravljanje informacijske varnosti in ustrezajo večini organizacij. Podrobneje so pojasnjene v nadaljevanju pod naslovom "Izhodišče informacijske varnosti".

Več informacij o izbiranju kontrol in drugih možnostih obravnavanja tveganja je mogoče najti v točki 4.2 Obravnavanje varnostnih tveganj.

0.6 Izhodišče informacijske varnosti

Število kontrol je mogoče obravnavati kot dobro izhodišče za izvajanje informacijske varnosti. Kontrole temeljijo na bistvenih zakonodajnih zahtevah ali pa so del splošne prakse za informacijsko varnost.

Kontrole, ki naj bi bile bistvene za organizacijo z zakonodajnega vidika, vključujejo glede na ustrezno zakonodajo:

- a) varovanje podatkov in zasebnost osebnih podatkov (glej 15.1.4),
- b) zaščito organizacijskih zapisov (glej 15.1.3),
- c) pravice intelektualne lastnine (glej 15.1.2).

Kontrole, sprejete kot splošna praksa za informacijsko varnost, vključujejo:

- a) dokument o informacijski varnostni politiki (glej 5.1.1),
- b) dodelitev odgovornosti za informacijsko varnost (glej 6.1.3),
- c) ozaveščenost o informacijski varnosti, izobraževanje in usposabljanje (glej 8.2.2),
- d) pravilno obdelavo v aplikacijah (glej 12.2),
- e) tehnično upravljanje ranljivosti (glej 12.6),
- f) upravljanje neprekinjenega poslovanja (glej 14),
- g) upravljanje incidentov informacijske varnosti in izboljšave (glej 13.2).

Te kontrole ustrezajo večini organizacij in večini okolij.

Naj velja opozorilo, da čeprav so vsi ukrepi v tem standardu pomembni in naj se upoštevajo, naj se določi primernost vsake kontrole v luči specifičnih tveganj, s katerimi se organizacija sooča. Zato je gornji pristop lahko dobro izhodišče, ampak ne nadomešča izbire kontrol na podlagi ocenjevanja tveganja.

0.7 Ključni dejavniki uspeha

Izkušnje so pokazale, da so naslednji dejavniki pogosto ključnega pomena za uspešno izvajanje informacijske varnosti v organizaciji:

- a) informacijska varnostna politika, cilji in aktivnosti, ki odražajo poslovne cilje,
- b) pristop in okvir za izvajanje, vzdrževanje, spremljanje in izboljševanje informacijske varnosti, ki je v skladu z organizacijsko kulturo,
- c) vidna podpora in zavezanost na vseh ravneh vodstva,
- d) dobro razumevanje zahtev informacijske varnosti, ocenjevanja in obvladovanja tveganja,
- e) uspešno trženje informacijske varnosti vsem vodjem, zaposlenim in drugim strankam za doseganje ozaveščenosti,
- f) razdeljevanje napotkov o politiki in standardih informacijske varnosti vsem vodjem, zaposlenim in drugim strankam,
- g) zagotavljanje financiranja dejavnosti upravljanja informacijske varnosti,
- h) zagotavljanje ustreznega ozaveščanja, usposabljanja in izobraževanja,
- i) vzpostavitev uspešnega procesa upravljanja informacijskih varnostnih incidentov,
- j) izvajanje sistema merjenja¹, ki se uporablja za vrednotenje delovanja upravljanja informacijske varnosti in daje povratne predloge za izboljšanje,
- k) upravljanje informacijske varnosti in povratne informacije predlogov za izboljšave.

0.8 Razvijanje lastnih smernic

Ta pravila obnašanja 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, je morda koristno vključiti sklice na točke v tem standardu, kjer je to primerno, kar bo olajšalo preverjanje skladnosti presojevalcem in poslovnim partnerjem.

¹ Upoštevajte, da merjenja informacijske varnosti niso vključena v področje uporabe tega standarda.

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

1 Področje uporabe

Ta mednarodni standard določa smernice in splošna načela za začetek, izvajanje, vzdrževanje in izboljševanje upravljanja informacijske varnosti v organizaciji. Cilji, opisani v tem mednarodnem standardu, so zagotoviti glavne smernice splošno uveljavljenih ciljev upravljanja informacijske varnosti.

Cilji kontrol in kontrole tega mednarodnega standarda naj bi se izvedli za izpolnitev zahtev, ki so bile prepoznane z ocenjevanjem tveganja. Ta mednarodni standard lahko služi kot praktična smernica za razvoj organizacijskih varnostnih standardov in praks uspešnega upravljanja varnosti ter kot pomoč pri gradnji zaupanja v medorganizacijskih aktivnostih.

2 Izrazi in definicije

V tem dokumentu so uporabljeni naslednji izrazi in definicije.

2.1

dobrina

kar koli, kar ima vrednost za organizacijo

[ISO/IEC 13335-1:2004]

2.2

kontrola

načini obvladovanja tveganja, vključno s politikami, postopki, smernicami, praksami ali organizacijskimi strukturami, ki so po naravi lahko upravni, tehnični, upravljalni ali pravni

OPOMBA: Kontrola se uporablja tudi kot sopomenka za ukrep ali protiuukrep.

2.3

smernica

opis, ki pojasnjuje, kaj naj se stori in kako, da se dosežejo cilji, določeni v politikah

[ISO/IEC 13335-1:2004]

2.4

naprave za obdelavo informacij

kakršen koli sistem, storitev ali infrastruktura za obdelavo informacij ali fizične lokacije, kjer se le-ta nahaja

2.5

informacijska varnost

ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij, dodatno so lahko vključene tudi druge lastnosti, kot so verodostojnost, odgovornost, neznanikanje in zanesljivost

2.6

informacijski varnostni dogodek

Informacijski varnostni dogodek je prepoznano dogajanje v sistemu, storitvi ali omrežju, ki kaže na morebitno kršitev informacijske varnosti, politike ali odpoved zaščitnih ukrepov ali na do tedaj še neznano okoliščino, ki je lahko pomembna za varnost

[ISO/IEC TR 18044:2004]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ISO/IEC 27002:2008

<https://standards.iteh.ai/catalog/standards/sist/080e09-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

2.7

informacijski varnostni incident

informacijski varnostni incident je določen z enim ali več neželenimi ali nepričakovanimi informacijskimi varnostnimi dogodki, ki predstavljajo veliko verjetnost ogrožanja poslovanja in informacijske varnosti

[ISO/IEC TR 18044:2004]

2.8

politika

celovit namen in usmeritev, kot ju formalno izrazi vodstvo

2.9

tveganje

kombinacija verjetnosti dogodka in njegove posledice

[ISO/IEC Vodilo 73:2002]

2.10

analiza tveganja

sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja

[ISO/IEC Vodilo 73:2002]

2.11

ocenjevanje tveganja

celovit proces analize tveganja in vrednotenja tveganja

[ISO/IEC Vodilo 73:2002]

2.12

vrednotenje tveganja

proces primerjave ocenjenega tveganja s kriteriji tveganja, da se določi pomembnost tveganja

[ISO/IEC Vodilo 73:2002]

2.13

obvladovanje tveganja

uskklajene aktivnosti organizacije za usmerjanje in nadzor tveganja

OPOMBA: Obvladovanje tveganja na splošno vključuje ocenjevanje tveganja, obravnavanje tveganja, sprejetje tveganja in obveščanje o tveganju.

[ISO/IEC Vodilo 73:2002]

2.14

obravnavanje tveganja

postopek izbire in izvedbe ukrepov za spremembo tveganja

[ISO/IEC Vodilo 73:2002]

2.15

tretja stranka

oseba ali organ, ki je glede na zadevno vprašanje priznan kot neodvisen od vpletenih strani

[ISO/IEC Vodilo 2:1996]

2.16

grožnja

možen vzrok neželenega incidenta, ki lahko povzroči škodo sistemu ali organizaciji

[ISO/IEC 13335-1:2004]

2.17

ranljivost

slabost dobrine ali skupine dobrin, ki jo lahko izkoristi ena ali več groženj

[ISO/IEC 13335-1:2004]

3 Struktura tega standarda

Ta standard vsebuje 11 točk o varnostnih kontrolah, ki skupaj tvorijo 39 glavnih varnostnih kategorij, in uvodno poglavje, ki predstavlja ocenjevanje in obravnavanje tveganja.

3.1 Točke

Vsaka točka vsebuje več glavnih varnostnih kategorij. Enajst točk (opremljenih s številom glavnih varnostnih kategorij, vključenih v posamezni točki) je:

- a) Varnostna politika (1),
- b) Organiziranje informacijske varnosti (2),
- c) Upravljanje dobrin (2),
- d) Varnost človeških virov (3),
- e) Fizična in okoljska varnost (2),
- f) Upravljanje komunikacij in delovanja (10),
- g) Nadzor dostopa (7),
- h) Pridobivanje, razvoj in vzdrževanje informacijskih sistemov (6),
- i) Upravljanje informacijskih varnostnih incidentov (2),
- j) Upravljanje neprekinjenega poslovanja (1),
- k) Skladnost (3).

OPOMBA: Vrstni red točk v tem standardu ne nakazuje njihove pomembnosti. Vse točke so lahko pomembne, odvisno od okoliščin, zato naj vsaka organizacija, ki uporablja ta standard, določi, kako pomembne so in njihovo uporabo v posameznih poslovnih procesih. Prav tako tudi noben seznam v tem standardu ni zapisan v prednostnem vrstnem redu, razen, če je tako navedeno.

3.2 Glavne varnostne kategorije

Vsaka glavna varnostna kategorija vsebuje:

- a) cilj kontrole, ki navaja, kaj je treba doseči, ter
- b) eno ali več kontrol, ki jih je mogoče uporabiti za doseganje cilja kontrole.

Opisi kontrole so strukturirani na naslednji način:

Kontrola

Določa specifične kontrolne izjave za izpolnitev cilja kontrole.