SLOVENSKI STANDARD

SIST ISO/IEC 27002

november 2013

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

Information technology – Security techniques – Code of practice for information security controls

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

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27002:2013 (sl)

Nadaljevanje na straneh od 2 do 84

NACIONALNI UVOD

Standard SIST ISO/IEC 27002 (sl), Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti, 2013, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27002 (en), Information technology – Security techniques – Code of practice for information security management, druga izdaja, 2013-10-01.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27002:2013 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 27002:2013 je prevod mednarodnega standarda ISO/IEC 27002:2013. V primeru spora glede besedila slovenskega prevoda je odločilen izvirni mednarodni standard v angleškem jeziku. Slovenski standard SIST ISO/IEC 27002:2013 je pripravil tehnični odbor SIST/TC ITC Informacijska tehnologija.

Odločitev za izdajo tega standarda je dne 25. oktobra 2013 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

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

SIST ISO/IEC 27000 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27002:2013

PREDHODNA IZDAJA

– SIST ISO/IEC 27002:2008

OPOMBI

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27002:2013 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

VSEBINA **Stran**

Predgovor

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 JTC ISO/IEC 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.

Napotki za izvajanje
Odgovornosti za informacijsko varnost naj se dodelijo v skladu z informacijskimi varnostnimi politikami (glej 5.1.1). Prepoznajo naj se odgovornosti za zaščito posameznih dobrin in za izvajanje specifičnih procesov informacijske varnosti. Določijo naj se odgovornosti za aktivnosti upravljanja z informacijskimi varnostnimi tveganji in še posebej za sprejemanje preostalih tveganj. Te odgovornosti naj se dopolnijo, kadar je to potrebno, s podrobnejšimi navodili za specifična mesta in naprave za obdelavo informacij. Lokalne odgovornosti za zaščito dobrin in za izvajanje specifičnih varnostnih procesov naj se jasno določijo.

Posamezniki z dodeljenimi odgovornostmi za informacijsko varnost bodo mogoče prenesli naloge varovanja na druge. Kljub temu ostanejo odgovorni in naj skrbijo, da so vse prenesene naloge pravilno opravljene.

Področja, za katera so posamezniki odgovorni, naj se navedejo. Stori naj se predvsem naslednje:

a) prepoznajo in opredelijo naj se dobrine in procesi informacijske varnosti;

b) vsaki dobrini ali procesu informacijske varnosti naj se dodeli odgovorna oseba, podrobnosti te odgovornosti naj se dokumentirajo (glej 8.1.2);

c) ravni odobritev naj se določijo in dokumentirajo;

d) dodeljeni posamezniki naj bodo usposobljeni na področju informacijske varnosti, da lahko izpolnijo svoje obveznosti, poleg tega naj jim bo omogočeno, da spremljajo razvoj tega področja;

e) prepoznana in dokumentirana naj bosta koordinacija in nadzor nad informacijskimi varnostnimi vidiki odnosov z dobavitelji.

Druge informacije

Mnoge organizacije imenujejo vodje informacijske varnosti, ki prevzamejo krovno odgovornost za razvoj in izvajanje informacijske varnosti ter podpirajo prepoznavanje kontrol.

Vendar pa bo odgovornost za pridobivanje virov in izvedbo kontrol pogosto ostala pri posameznih vodjih. Pogosta praksa je, da se vsaki dobrini določi lastnik, ki nato postane odgovoren za njeno redno dnevno zaščito.

6.1.2 Razmejitev dolžnosti

Kontrola
Nasprotujoče si naloge in področja odgovornosti naj se razmejijo, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo dobrin organizacije.

Napotki za izvajanje
Potrebna je previdnost, da nobena posamezna oseba ne more dostopati, spreminjati ali uporabljati dobrin brez dovoljenja ali neopazno. Začetek dogodka naj se loči od njegove odobritve. Pri snovanju kontrol naj se upošteva možnost dogovarjanja.

V majhnih organizacijah je razmejitev dolžnosti morda težko doseči, vendar pa naj se načelo uporablja, kolikor je to mogoče in izvedljivo. Kadar je razmejevanje težko, naj se razmisli o drugih kontrolah, kot so spremljanje aktivnosti, revizijske sledi in nadzor vodstva.

Druge informacije
Razmejitev dolžnosti je metoda za zmanjšanje tveganj naključne ali namerne zlorabe dobrin organizacije.

6.1.3 Stik s pristojnimi organi

Kontrola
Vzdržujejo naj se ustrezni stiki s pristojnimi organi.

Napotki za izvajanje
Organizacije naj imajo na voljo postopke, ki določajo, kdaj in kdo naj stopi v stik z organi (npr. pooblaščenimi osebami za kazenski pregon, regulatornimi in nadzornimi organi) ter kako naj se ugotovljeni informacijski varnostni incidenti pravočasno prijavljajo (npr. če obstaja sum kršenja zakonov).

Druge informacije
Organizacijam, napadenim prek interneta, bodo morda morali pri izvedbi ukrepov proti izvoru napada pomagati pristojni organi.

Vzdrževanje takšnih stikov je lahko zahteva za podporo upravljanju informacijskih varnostnih incidentov (glej točko 16) ali neprekinjenega poslovanja in procesa načrtovanja nepredvidljivih dogodkov (glej točko 17). Stiki z regulatornimi organi so prav tako koristni za predvidevanje in pripravo na prihajajoče spremembe zakonov ali predpisov, ki jih mora organizacija izvajati. Stiki z drugimi organi obsegajo komunalne službe, reševalne službe, električne dobavitelje, službe, odgovorne za zdravje in varnost, npr. gasilske enote (v zvezi z neprekinjenim poslovanjem), telekomunikacijske ponudnike (v zvezi z usmerjanjem povezav in razpoložljivostjo) in dobavitelje vode (v zvezi s hladilnimi sistemi za opremo).

6.1.4 Stik s specifičnimi interesnimi skupinami

Kontrola
Vzdržujejo naj se ustrezni stiki s specifičnimi interesnimi skupinami ali z drugimi strokovnimi forumi in združenji za varnost.

Napotki za izvajanje

Članstvo v specifičnih interesnih skupinah ali forumih naj se obravnava kot sredstvo za:

a) izboljševanje znanja o najboljših praksah ter spremljanje ustreznih novih informacij o varnosti,

b) zagotavljanje tekočega in popolnega razumevanja okolja informacijske varnosti,

c) prejemanje zgodnjih opozoril, nasvetov in popravkov, ki se nanašajo na napade in ranljivosti,

d) pridobivanje dostopa do strokovnih nasvetov glede informacijske varnosti,

e) razširjanje in izmenjavo informacij o novih tehnologijah, izdelkih, grožnjah ali ranljivostih,

f) zagotavljanje ustreznih točk povezave pri ravnanju z informacijskimi varnostnimi incidenti (glej točko 16).

Druge informacije
Vzpostaviti je mogoče dogovore o delitvi informacij, ki izboljšajo sodelovanje in usklajevanje varnostnih vprašanj. Taki dogovori naj prepoznajo zahteve za zaščito občutljivih informacij.

6.1.5 Informacijska varnost v upravljanju projektov

Kontrola
Informacijska varnost naj bo obravnavana v okviru upravljanja projektov ne glede na vrsto projekta.

Napotki za izvajanje
Informacijska varnost naj bo vključena v metode upravljanja projektov organizacije, da se zagotovi, da so informacijska varnostna tveganja prepoznana in upoštevana kot del projekta. To v splošnem velja za vsak projekt ne glede na vrsto, npr. projekt za osnovne poslovne procese, informacijsko tehnologijo, upravljanje objektov in druge podporne procese. Uporabljene metode upravljanja projektov naj zahtevajo, da:

a) so cilji informacijske varnosti vključeni v cilje projekta;

b) je v zgodnji fazi projekta izdelana ocena informacijskih varnostnih tveganj, da se prepoznajo potrebne kontrole;

c) je informacijska varnost del vseh faz uporabljene metodologije projekta.

Posledice informacijske varnosti naj se pri vseh projektih redno obravnavajo in pregledujejo. Odgovornosti za informacijsko varnost naj bodo določene in dodeljene posebnim vlogam, ki so določene v metodah upravljanja projektov.

6.2 Mobilne naprave in delo na daljavo

Cilj: Zagotoviti varnost dela na daljavo in uporabe mobilnih naprav.

6.2.1 Politika na področju mobilnih naprav

Kontrola
Sprejmejo naj se politika in podporni varnostni ukrepi za upravljanje tveganj, nastalih z uporabo mobilnih naprav.

Napotki za izvajanje
Pri uporabi mobilnih naprav naj se posebna pozornost posveti zagotovitvi, da niso zlorabljene poslovne informacije. Politika mobilnih naprav naj upošteva tveganja pri delu z mobilnimi napravami v nezaščitenih okoljih.

Politika mobilnih naprav naj obravnava:

a) registracijo mobilnih naprav,

b) zahteve za fizično zaščito,

c) omejitve pri nameščanju programske opreme,

d) zahteve za različice programske opreme mobilne naprave in za nameščanje popravkov,

e) omejitve povezave do informacijskih storitev,

f) kontrole dostopa,

g) kriptografske tehnike,

h) zaščito pred zlonamerno programsko opremo,

i) oddaljeno onemogočanje, brisanje ali zaklepanje,

j) varnostne kopije,

k) uporabo spletnih storitev in aplikacij.

Previdno naj se ravna pri uporabi mobilnih naprav na javnih mestih, v sejnih sobah in drugih nezaščitenih območjih. Uvedena naj bo zaščita pred nepooblaščenim dostopom ali razkritjem informacij, shranjenih in obdelanih v teh napravah, na primer z uporabo kriptografskih tehnik (glej točko 10), in uporabljene naj bodo tajne informacije za preverjanje verodostojnosti (glej 9.2.4).

Mobilne naprave naj se tudi fizično zaščitijo pred krajo, zlasti kadar so nenadzorovane, na primer v avtomobilih in drugih oblikah prevoza, hotelskih sobah, konferenčnih centrih in na mestih srečanj. Ob upoštevanju pravnih, zavarovalnih in drugih varnostnih zahtev organizacije naj se vzpostavi poseben postopek za primere kraje ali izgube mobilnih naprav. Naprave, ki fizično prenašajo pomembne, občutljive ali kritične poslovne informacije, naj ne ostanejo brez nadzora, in kjer je to mogoče, naj bodo fizično zaklenjene ali pa naj se uporabijo posebne ključavnice za zavarovanje naprav.

Za osebje, ki uporablja mobilne naprave, naj se organizira izpopolnjevanje za dvig njihove ozaveščenosti o dodatnih tveganjih, ki izhajajo iz takšnega načina dela, in o kontrolah, ki naj se izvajajo.

Kjer politika mobilnih naprav dovoljuje uporabo mobilnih naprav v zasebni lasti, morajo ta politika in povezani varnostni ukrepi upoštevati tudi: