Varnostna politika informacijskega sistema za potrebe ISO 27001

1 Varnostna politika informacijskega sistema

1.1 Splošni del

Cilj informacijske varnosti je zagotoviti nemoteno in varno poslovanje družbe in zmanjšati škodo s preprečitvijo in zmanjšanjem posledic neželenih informacijskih varnostnih dogodkov.

Namen varnostne politike je zaščita informacijskih sredstev in virov družbe pred vsemi nevarnostmi, notranjimi ali zunanjimi, namernimi ali nenamernimi.

Varnostna politika predstavlja na enem mestu zbrana navodila ter standarde za zagotavljanje in upravljanje z informacijsko varnostjo za vse uporabnike informacijskega sistema.

Podjetje s številnimi kontrolnimi mehanizmi in ustaljeno strukturo odgovornosti, procesov in postopkov zagotavlja, da je informacijska varnost sestavni del vseh poslovnih procesov, operacij in sistemov upravljanja. Ta dokument prikazuje obvezo uprave podjetja da vzpostavi, implementira, izvaja, nadzira, preverja, vzdržuje in izboljšuje sistem upravljanja informacijske varnosti.

Informacijska varnostna politika obsega:

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij,
- varovanje informacij pred nepooblaščenim dostopom, razkritjem, spremembo ali uničenjem,
- zagotavljanje izobraževanja o informacijski varnosti vseh zaposlenih,
- seznanjanje s pravili varne uporabe za vse uporabnike informacijske infrastrukture družbe,
- obvladovanje vseh varnostnih incidentov ter ustrezno ukrepanje,
- izpolnjevanje usklajenosti z zakoni in predpisi.

Vsi, ki imajo dostop do informacijskega sistema podjetja, morajo izpolnjevati zahteve informacijske varnostne politike, saj so za uresničevanje ciljev informacijske varnosti na svojem delovnem področju odgovorni vsi zaposleni v podjetju.

Odgovorna oseba, ki koordinira delo z zunanjimi izvajalci, je zadolžena, da se zunanji izvajalec seznani z varnostno politiko in upošteva njena določila. Zunanji izvajalec mora pred pričetkom del podpisati izjavo o seznanitvi in izpolnjevanju določil informacijske varnostne politike.

1.1.1 Vodstvo

Vodstvo družbe mora zagotoviti, da zaposleni izpolnjujejo zahteve informacijske varnostne politike. Odgovorno je za zavrnitev neupravičenih ali nepotrebnih zahtev po dostopu do informacijskih virov ter za zagotavljanje ukinitve dostopa do informacijskih virov, ko ga zaposleni ne potrebujejo več.

Vodstvo je odgovorno za učinkovito upravljanje z informacijsko varnostjo. V ta namen izvaja vodstvene preglede učinkovitosti sistema za upravljanje z varnostjo, ki obsegajo preglede:

- rezultatov revizij in pregledov sistema,
- poročila ocene tveganja in identificiranih groženj,
- poročila o spremembah, ki lahko vplivajo na informacijsko varnost,
- predlogov za izboljšave.

V okviru svojega dela ima vodstvo tudi naslednje zadolžitve:

- potrjuje strateške smernice za informacijsko varnost,
- odloča o merilih za sprejemanje tveganja in o sprejemljivi ravni tveganja za informacijsko varnost znotraj obsega in meja ISMS,
- potrjuje dokumente informacijske varnostne politike,
- pomaga pri uvajanju večjih projektov informacijske varnosti,
- nadzira večje spremembe pri izpostavljenosti informacijskih sredstev varnostnim grožnjam,
- nadzira in ocenjuje varnostno učinkovitost in zmogljivost.

Odgovorna oseba za informacijsko varnost je zadolžena za učinkovito izvajanje informacijske varnosti v družbi.

1.1.2 Odgovorna oseba za informacijsko varnost

Naloge odgovorne osebe za informacijsko varnost so:

- poročanje vodstvu o vseh zadevah, povezanih z informacijsko varnostjo,
- svetovanje o vseh področjih, ki so povezana z informacijsko varnostjo,
- usklajevanje izvajanja varnostnih ukrepov na vseh ravneh ter poročanje poslovodstvu o njihovi učinkovitosti,
- začetek in usklajevanje ocenjevanja in upravljanja tveganj za informacijsko varnost,
- pregled in posodabljanje kataloga tveganj,
- pregled in posodabljanje kataloga sprememb v IT infrastrukturi in kataloga varnostnih incidentov,
- vodenje, posodabljanje in pregledovanje registra dobrin (informacijskih virov),
- razvoj varnostne politike in nadzorstev,
- redni pregled in po potrebi posodobitev politik informacijske varnosti vsaj enkrat letno, vključno s pregledom ustreznosti pogodb o zaposlitvi v zvezi z informacijsko varnostjo,
- izredni pregled in po potrebi posodobitev politik informacijske varnosti ob spremembah v informacijskem sistemu, ki povečujejo tveganja na podlagi ocene, izdelane v okviru upravljanja projektov, sprememb ali iz drugih razlogov, ki zahtevajo oceno tveganja,
- vzdrževanje in izboljšanje metodologij in procesov upravljanja informacijske varnosti,
- nadzor izvajanja varnostne politike in nadzorstev,
- zagotavljanje rednih pregledov notranjih revizij ISMS,
- zagon načrtov in programov za ohranjanje ozaveščenosti o pomembnosti informacijske varnosti,
- prepoznavanje in poročanje o incidentih, ranljivosti in grožnjah, ki niso bile ustrezno obravnavane v dejavnostih upravljanja s tveganji,
- kontaktiranje in usklajevanje postopkov s pristojnimi organi, kadar je to potrebno zaradi varnostnega incidenta, za katerega je potrjeno, da vpliva na skladnost in je poročanje o incidentu glede na okoliščine incidenta pristojnemu organu obvezno.

1.1.3 Notranji revizor sistema upravljanja informacijske varnosti

So pooblaščeni in odgovorni za izvajanje notranjih revizij ISMS ter poročanje upravi in vodjem procesov o rezultatih revizij v skladu s postopkom, opisanim v dokumentu Postopek notranjega preverjanja ISMS.

1.1.4 Lastnik informacijskega sredstva

Lastnik informacijskega sredstva je odgovoren za nadzor, razvoj, vzdrževanje in varovanje informacijskega sredstva družbe.

1.1.5 Naloge lastnika informacijskega sredstva so:

- potrjevanje upravičenosti dostopa za posamezne uporabnike ob zahtevi za dostop,
- pregled uporabnikov s pooblastili za dostop do informacijskega vira (enkrat letno),
- pregled uporabnikov s posebnimi (administrativnimi) pooblastili dostopa v rednih časovnih intervalih (vsakih 6 mesecev).

1.1.6 Skrbnik informacijskega vira in komunikacijske infrastrukture

Skrbnik je zadolžen za vzpostavitev delovanja, nastavitve in vzdrževanje informacijskih virov in komunikacijske infrastrukture družbe.

Naloge skrbnika so:

- pregled varnostnih dogodkov v dnevniških zapisih in ukrepanje v primeru zaznanih nepravilnosti,
- preverjanje delovanja informacijskega vira in komunikacijske infrastrukture,
- vpeljava in vzdrževanje informacijskih rešitev z namenom zagotavljanja nemotenega delovanja informacijskega vira ali komunikacijske infrastrukture,
- implementacija varnostnih nastavitev za informacijski vir ali komunikacijsko infrastrukturo,
- odprava napak v delovanju in raziskovanje vzrokov za motnje v delovanju,
- stalno izobraževanje z namenom osveževanja znanja na področju dela, ki ga opravlja skrbnik.

1.1.7 Uporabniki informacijskega sistema

Vsi zaposleni, obiskovalci in drugi uporabniki informacijskega sistema, vključno z zunanjimi izvajalci, morajo upoštevati informacijsko varnostno politiko.

1.2 Izjava o politiki ISMS

Poslovodstvo podjetja je sprejelo odločitev za vzpostavitev, implementacijo, izvajanje, nadzor, preverjanje, vzdrževanje in izboljšanje sistema upravljanja informacijske varnosti za zadostno in z najvišjimi mednarodnimi standardi skladno obvladovanje tveganj informacijske varnosti.

Z zavezanostjo k vzpostavitvi ISMS si prizadevamo dokazati zaposlenim, strankam in poslovnim partnerjem, da skrbimo za (njihovo) informacijsko varnost ob upoštevanju relevantnih poslovnih, pravnih in pogodbenih obveznosti, vezanih na informacijsko varnost.

Vodstvo podjetja s politiko ISMS izkazuje odločnost in pripravljenost za zaščito celotnega informacijskega premoženja v smislu njegove integritete, zaupnosti in razpoložljivosti ter pravnih in poslovnih interesov.

Cilji informacijske varnosti znotraj obsega in meja ISMS so: vzdrževanje tveganj informacijske varnosti na sprejemljivi ravni, učinkovito upravljanje informacijske varnosti, vzpostavitev in vzdrževanje učinkovitega sistema pristojnosti in odgovornosti za informacijsko varnost ter izpolnjevanje pogodbenih, zakonskih in regulativnih obveznosti glede informacijske varnosti .

Učinkovitost sistema upravljanja informacijske varnosti in implementiranih varnostnih nadzorov za zaščito informacijskega premoženja v obsegu in mejah ISMS se bo nenehno ocenjevala v skladu s strateškim kontekstom upravljanja tveganj.

Varnostni nadzor se bo uporabljal le, če je upravičen, funkcionalen, donosen in učinkovit.

Vsi zaposleni in zunanji sodelavci, ki sodelujejo v poslovnih procesih, morajo upoštevati to politiko, vsa druga dokumentirana navodila ter vse poslovne, pravne in regulativne zahteve za informacijsko varnost, ki so opredeljeni znotraj obsega in meja ISMS. Na ta način prevzemajo tudi delno odgovornost za informacijsko varnost in so v primeru kršitve politike varnosti in postopkov odgovorni v skladu s pogodbenimi obveznostmi in internimi pravili.

Redni nadzor nad izvajanjem politike sistema upravljanja informacijske varnosti se bo izvajal s pregledi dejavnosti ISMS (angl. »management review«) in s preverjanjem učinkovitosti izvedenih varnostnih kontrol.

1.3 Sodelovanje z interesnimi skupinami

Nismo vključeni v interesne skupine, zato v zvezi s sodelovanjem z interesnimi skupinami posebni postopki trenutno niso predvideni.

Vodstvo bo pozorno na morebitna združenja, ki bi lahko za družbo predstavljala dodano vrednost.

Ob rednih preverjanjih politike informacijske varnosti je treba spremeniti to podpoglavje, če se bo družba vključila v interesno združenje in opredeliti obveznosti in pogoje sodelovanja z združenjem ter pogoje za vodenje evidence združenj.

2 Varnostna politika za uporabnike informacijskega sistema

Uporaba računalniške informacijske opreme in infrastrukture družbe je namenjena samo za podporo rednim in izrednim delovnim procesom, ki jih izvaja družba (vsakodnevnemu delu, projektom in podpornim aktivnostim).

Vsak uporabnik sam prevzema vse posledice za nezakonito ali drugo nedovoljeno uporabo računalniške informacijske opreme družbe ali lastne računalniške opreme.

Uporaba elektronske pošte in interneta se dovoljuje in omejuje v skladu s politiko družbe in se regulira v smislu večanja varnosti in zmanjševanja informacijskih incidentov. Vse sistemske uporabniške aktivnosti se beležijo z namenom zagotavljanja nemotenega delovanja informacijskega sistema.

Informacijski sistem lahko na podlagi samodejnih mehanizmov prepreči dostop do nekaterih spletnih strani in internetnih storitev. Omejitve določi odgovorna oseba za informacijsko varnost in odobri vodstvo družbe.

Vsebina uporabniških aktivnosti, t.j. vsebina uporabnikovih paketov (vsebina e-pošte, vsebina priponk, vsebina obiskov internetnih strani), se ne beleži ali kako drugače spremlja z vpogledom v vsebine, ki se prenašajo.

Uporabnikom je dostop do interneta omogočen za njihovo delo in izobraževanje. Uporabnik se mora obnašati racionalno in internet uporabljati kot delovni pripomoček.

Uporaba storitev v oblaku za shranjevanje podatkov (npr. Dropbox) je dovoljena samo s predhodnim izrecnim soglasjem vodstva družbe. Izjema je uporaba elektronske pošte v oblaku, ki pa jo lahko uporabniki uporabljajo samo za osebna sporočila.

Uporaba komunikacij »vsak z vsakim« (angl. »peer to peer«), kot je npr. omrežje TOR, omrežje BitTorrent, ni dovoljena.

Uporaba komunikacijskih posrednikov (angl. »proxy«) izven nadzora družbe pri dostopu do interneta ni dovoljena.

Za vsak dostop v omrežje internet se lahko vodi evidenca v skladu z informacijsko varnostno politiko, ki je namenjena spremljanju uporabe interneta za statistične prikaze, za načrtovanje kapacitet strežnikov in za odkrivanje morebitnih zlorab. Ti podatki so tajni in razen IP naslova ne vsebujejo osebnih podatkov uporabnikov.

Pri vključitvi v omrežje in uporabi storitve ni dovoljeno uporabljati lažnih ali zavajajočih osebnih podatkov.

Nedopustno je pošiljati prispevke za nestrokovne ali osebne polemike, oglase, verižna sporočila ali izvajati katerekoli druge podobne aktivnosti, ki motijo delo drugih uporabnikov ali vplivajo na negativen ugled družbe.

Ni dovoljeno prenašati podatkov z žaljivo ali pornografsko vsebino, tajnih podatkov ali podatkov, ki so zaščiteni z avtorskimi pravicami ali so v lasti drugih uporabnikov.

Nedopustno je uničevanje ali spreminjanje podatkov, ki so last drugih uporabnikov, ter uporaba programov ali postopkov, ki ovirajo normalno delovanje informacijskih naprav, ki sestavljajo omrežje.

Lastnik informacijskega sredstva se lahko odloči za ukrepanje v primeru, če bi uporabnik:

- uporabljal javne konferenčne sisteme za komercialno oglaševanje,
- zmerjal, zasmehoval ali žalil druge uporabnike interneta (angl. "flaming"),
- ščuval k verski, rasni, spolni, nacionalni, politični ali kakšni drugi nestrpnosti,
- izvajal aktivnosti, ki lahko povzročijo pošiljanje velikih količin podatkov in privedejo do zavrnitve storitev (DoS in DDoS napad),
- izvajal aktivnosti, ki lahko privedejo do sprožitve velikega števila zahtev po vzpostavitvi povezav in s tem onemogočijo uporabo storitev drugim uporabnikom ("SYN attack").

V primeru nedovoljene uporabe storitev v internet omrežju lahko skrbnik uporabniku začasno onemogoči uporabo informacijskega sistema.

Posebna skrb mora biti posvečena uporabi programske opreme, ki je kot intelektualna lastnina zaščitena z avtorskimi pravicami. Pred nameščanjem programske opreme za ustrezno licenco poskrbijo lastniki informacijskih sredstev.

Večina informacij in programske opreme (glasba, video, programi, filmi, dokumenti, ...), ki so dostopni v javni domeni (vključno z internetom), je zaščitena z avtorskimi pravicami ali drugo obliko zaščite intelektualne lastnine. S kršenjem avtorskih pravic in intelektualne lastnine posameznik prevzame vso materialno in kazensko odgovornost. V primeru dvomov o možnosti uporabe materialov se je treba posvetovati s pristojno službo.

Če uporabnik potrebuje programsko opremo, ki ni del standardne, se za nakup in nameščanje opreme dogovori s predpostavljenim in lastnikom informacijskega sredstva.

Uporaba programske opreme, pridobljene na nelegalen način, je prepovedana.

Družba zbira in vzdržuje osebne podatke, ki so zbrane v zbirkah osebnih podatkov.

Osebne datoteke, informacije in podatke, ki jih uporabniki zbirajo pri opravljanju svojega dela, je potrebno vedno hraniti na za to predpisanih informacijskih sredstvih, ki so zavarovana.

Postopki varovanja so podrobneje določeni v pravilniku, ki ureja to področje.

Zaposleni ne smejo dostopati do informacijskih sredstev drugih zaposlenih (npr. datotek, zapisov, drugih vsebin na različnih napravah in v fizični obliki) brez predhodne odobritve lastnika oz. skrbnika (v primeru osebnih podatkov brez privolitve posameznika).

Zaposleni na informacijskih sredstvih družbe ne smejo shranjevati lastnih osebnih podatkov, ki se ne nanašajo na opravljanje poslov družbe.

2.1 Projektno vodenje

Vsak projekt, ki spreminja informacijski sistem, predstavlja spremembo informacijskega sistema, zato ga je treba obravnavati na enak način kot ostale spremembe v informacijskem sistemu, kot je določeno v tej politiki.

2.1.1 Ocenjevanje tveganja

Vsak projekt lahko vpliva na tveganja, povezana z zagotavljanjem varnosti informacijskega sistema. Upravljanje tveganj, povezanih s spremembami, je obravnavano v sklopu upravljanja sprememb informacijskega sistema, zato je treba vse spremembe, ne glede na to ali so vodene kot projekt, obravnavati skladno s postopku upravljanja sprememb informacijskega sistema, kot je določeno v tej politiki.

2.2 Varnost mobilnih naprav

Mobilne naprave (dlančniki, tablice, mobilni telefoni z dostopom do podatkov,...) in prenosni mediji (USB ključ, prenosni diski…) morajo imeti zagotovljeno fizično ali vsaj logično zaščito, ne glede na to, če so na njih shranjeni zaupni podatki.

Z mobilnimi napravami in prenosnimi mediji je potrebno ravnati tako, da je kolikor je glede na okoliščine mogoče, zmanjšana možnost odtujitve naprave ali medija in s tem shranjenih podatkov, zato jih ni dovoljeno odlagati na nezaščitenih in javnih prostorih, kjer so izpostavljeni možnosti odtujitve.

Uporabnik mora ravnati z mobilno napravo na način, ki onemogoča uporabo nepooblaščeni osebi, zato mora izvajati naslednje ukrepe:

- Naprave ne sme puščati na nenadzorovanem mestu brez nadzora.
- Kadar naprave ne uporablja, jo mora zakleniti.
- Kadar je to mogoče, mora biti naprava ob odsotnosti uporabnika fizično varovana – na poti v osebni torbi, aktovki, kovčku, v poslovnih prostorih v predalu ali omari, ki omogoča zaklepanje.

Skrbnik informacijskega vira mora zagotoviti, da so na mobilni napravi ali mediju aktivni naslednji varnostni ukrepi:

- Nastavljeno mora biti zaščitno geslo za vklop in časovno nadzorovan samodejni izklop ali zaklepanje na napravah, ki to omogočajo.
- Podatki na nosilcu podatkov, ki je vgrajen v napravo, morajo biti šifrirani.
- Podatki na prenosljivih nosilcih podatkov in nosilci podatkov v prenosnih napravah morajo biti zaščiteni s šifriranjem.

2.3 Delo na daljavo

Na naprave, ki jih uporabnik uporablja za delo na daljavo, mora namestiti najnovejše popravke programske opreme, predvsem pa ne odlašati z njihovo namestitvijo. To se nanaša tako na popravke operacijskega sistema (npr. Windows, Android, iOS) kot popravke ostale programske opreme (npr. pisarniški programi Microsoft Office, kot tudi aplikacije, ki jih je uporabnik namestil iz trgovine z aplikacijami ali drugega vira).

Če uporabnik na lastni računalniški opremi uporablja kakršnokoli piratsko programsko opremo, ki jo je pridobil z licenčnimi ključi ali celo namestitvenimi programi, dostopnimi v internetu (npr. v omrežju Torrent), na takšni računalniški opremi ne sme obdelovati osebnih podatkov.

Na lastno računalniško napravo, ki jo uporablja za obdelavo podatkov družbe, mora uporabnik namestiti protivirusno programsko opremo, če je še nima. Nekatere rešitve so na voljo brezplačno, npr. Windows Defender.

Na lastni računalniški napravi, ki jo uporablja za delo na daljavo, mora uporabnik vključiti požarni zid, še posebej, če je bil izklopljen ali so bile spremenjene njegove nastavitve. Če je uporabnik spreminjal njegove nastavitve, jih mora ponovno preveriti in se prepričati, da izbrane nastavitve zagotavljajo zadostno raven varnosti. Če uporabnik ni prepričan, katere nastavitve so ustrezne, uporabite privzete nastavitve. Večina požarnih zidov ima možnost za ponastavitev spremenjenih nastavitev.

Domači usmerjevalniki, naprave, ki jih praviloma zagotovijo ponudniki dostopa do interneta, omogočajo osnovno zaščito domačega omrežja. Če je uporabnik spremenil privzete nastavitve, se mora prepričati, ali spremenjene nastavitve zagotavljajo ustrezno raven varnosti uporabnikovega domačega omrežja. Če uporabnik ni prepričan katere nastavitve so ustrezne, mora uporabiti privzete nastavitve. Večina usmerjevalnikov ima možnost za ponastavitev spremenjenih nastavitev.

Podatkov informacijskega sistema družbe uporabnik praviloma ne sme shranjevati na lastnih napravah.

Kadar je le mogoče, mora uporabnik za obdelavo podatkov družbe uporabiti namenske programe, ki jih je zagotovil delodajalec (npr. računovodski program) ali shrambo v oblaku, ki jo je zagotovil delodajalec (npr. OneDrive).

Pri uporabi shrambe v oblaku, jo mora uporabnik, če je le tehnično mogoče, nastaviti tako, da bodo podatki shranjeni le v oblaku in ne na nosilcu podatkov v napravi uporabnika.

Če mora uporabnik zaradi narave dela nujno shraniti podatke na lastni računalniški napravi, mora sproti zmanjševati obseg podatkov, ki so shranjeni na napravi in se omejiti le na tiste, ki jih trenutno nujno potrebuje pri svojem delu. Ko z delom konča, mora podatke, ki zahtevajo hrambo, če je le mogoče čim prej prenesti v varno hrambo organizacije in na lastni računalniški napravi podatke izbrisati.

Če je le tehnično mogoče, mora uporabnik shranjevati podatke na lastni računalniški napravi na šifriranem nosilcu podatkov. V Windows je temu namenjena funkcionalnost BitLocker, prav tako šifriranje nosilca podatkov omogoča večina sodobnih prenosnih naprav (mobilnih telefonov in tablic), ne glede na operacijski sistem (Android, iOS).

Če uporabnik na nosilcu podatkov ni vključil šifriranja podatkov, naprave, na kateri je shranil osebne podatke, ne sme iznašati iz prostorov. Velja tudi za USB ključke in druge naprave za hrambo podatkov (npr. prenosne diske). V tem primeru mora uporabnik glede na razpoložljive možnosti uporabiti dodatne mehanizme varovanja, npr. zakleniti napravo oziroma nosilec podatkov v delovno sobo ali vsaj omaro/predal, kadar je ne uporablja.

Če uporabnik shranjuje podatke družbe na lastni napravi, je sam odgovoren za to, da poskrbi, da podatkov ne bi namerno ali nenamerno izgubil (nenameren izbris, uničenje naprave ipd.). V tem primeru je uporabnik dolžen izdelati varnostno kopijo podatkov. Varnostno kopijo mora fizično zaščititi (po

kopiranju mora uporabnik odklopiti nosilec podatkov od naprave in ga shraniti na varnem, če je le mogoče, zaklenjenem mestu).

Podatkov družbe uporabnik ne sme prenašati brez šifriranja. Če uporabnik uporablja namenske spletne aplikacije, lahko preveri ali je povezava šifrirana, če je v levem kotu vrstice v brskalniku, v kateri je prikazan naslov spletne strani, prikazana ključavnica.

Uporabnik se mora zavedati, da varna brezžična (Wifi) povezava ne nadomešča šifriranja pri prenosu podatkov, še posebej v primeru, če za povezavo z internetom uporablja tujo brezžično povezavo.

Vzpostavitev navideznega zasebnega omrežja (VPN povezave) zagotavlja šifriranje podatkov med napravo, ki jo uporablja uporabnik in omrežjem organizacije in je zato praviloma ustrezna in varna rešitev za delo na daljavo. Če je to tehnično mogoče, ga mora uporabnik uporabiti.

Če uporabnik za oddaljeno delo uporablja oddaljeno namizje (npr. vgrajeno v Microsoft Windows, TeamViewer ali podobne rešitve), se mora zaradi varne nastavitve požarnega zidu in povezljivosti z oddaljenim računalnikom posvetovati s skrbnikom informacijskega vira in tega na službenem računalniku ne sme vzpostavljati sam, če ni za to pooblaščen.

2.4 Usposabljanje uporabnikov

Vsi uporabniki informacijskega sistema se morajo redno izobraževati s področja informacijske varnosti, najmanj ob rednem izobraževanju na področju varstva pri delu in požarne varnosti.

Pri izvedbi izobraževanja morajo biti kot gradiva uporabljene zadnje različice varnostnih politik, navodil, predpisov in drugih virov, na katere se nanaša izobraževanje.

2.5 Postopek razvrščanja informacij

Postopek in ravni razvrščanja informacij so opredeljeni.

2.6 Ravnanje z nosilci podatkov/informacij

Zaupne informacije družbe morajo biti varovane pred nepooblaščenim dostopom, pregledom in spreminjanjem:

- Zaupne informacije družbe morajo biti praviloma šifrirane ob pošiljanju izven omrežja družbe.
- Zaupne informacije na prenosnih medijih (zgoščenke, prenosni trdi diski, USB ključi…) je potrebno označiti kot zaupne in hraniti v ustreznih prostorih ali omarah. Zaupni podatki se shranjujejo na prenosne nosilce podatkov samo izjemoma.
- Zaupne informacije družbe ne smejo biti shranjene na računalnikih, ki niso v lasti družbe.
- Pri tiskanju zaupnih informacij družbe je dovoljeno uporabljati le interne tiskalnike. Tiskani material je potrebno takoj pobrati in varno hraniti.
- Po prenehanju uporabe natisnjenih dokumentov oz. drugih medijev, ki vsebujejo zaupne informacije, je potrebno medije fizično uničiti ali podatke izbrisati na način, ki onemogoča obnovitev izvirnih informacij (razrez tiskanih medijev, fizično uničenje nosilcev kot so CD, DVD, večkratni prepis pomnilniškega medija z naključnimi vrednostmi).

Pravila ravnanja z nosilci podatkov/informacij so opredeljena v dokumentu 14.

2.7 Nadzor dostopa

Pravila kontrole dostopa so opredeljena v dokumentu 15.

2.8 Upravljanje gesel

Pravila upravljanja gesel so opredeljena v dokumentu16.

2.9 Uporaba posebnih pomožnih programov

Uporaba posebnih pomožnih programov, ki bi lahko spremenili sistemske in aplikacijske kontrole, je prepovedana.

2.10 Dostop do izvorne kode

Do izvorne kode lahko dostopajo le razvijalci programske opreme.

Izvorna koda mora biti shranjena v odložišču izvorne kode.

Odložišče izvorne kode mora omogočati kontrolo dostopa.

Odložišče izvorne kode mora zagotavljati revizijsko sled sprememb izvorne kode.

Zagotovljena mora biti povezava med posamezno spremembo izvorne kode in zahtevkom za spremembo, na podlagi katerega je sprememba izvorne kode nastala.

2.11 Kriptografija

Pravila uporabe kriptografskih kontrol so opredeljena v dokumentu 1.

2.12 Fizična in okoljska varnost

2.12.1 Fizična varnost

Cilj fizične zaščite je preprečiti nepooblaščen fizični dostop, škodo in motnje v prostorih, ter preprečiti izgubo, škodo, krajo ali kompromitiranje informacijskih sredstev.

Glavna vhodna vrata v poslovno stavbo so izven delovnega časa zaklenjena.

Vhodna vrata v poslovni prostor družbe so izven delovnega časa zaklenjena.

V delovnem času, ko so vhodna vrata v poslovni prostor odklenjena, vstop v prostore nadzoruje tajništvo.

Področje fizičnega varovanja obsega poslovno stavbo in poslovni prostor družbe.

Odgovorna oseba za informacijsko varnost vodi evidenco ključev.

2.12.2 Okoljska varnost

Osnovno fizično zaščito opreme pred poškodbami zagotavlja fizično varovanje.

Za druge vrste okoljskih tveganj, izrecno požar, poplava, udar strele, potres, vlom, mora imeti družba sklenjeno ustrezno zavarovanje opreme pri zavarovalnici.

2.13 Zaščita opreme

Oprema, ki zagotavlja delovanje informacijskega sistema ali se uporablja v poslovnih prostorih, kot je električno napajanje, telekomunikacije, vodovod, plin, kanalizacija, prezračevanje in klimatizacija, morajo biti nameščeni skladno z zahtevami proizvajalca.

Za opremo, za katero proizvajalec zahteva redne preglede, morajo biti pregledi dokumentirani in izvedeni skladno z navodili proizvajalca.

Lokacije nujnih stikal in ventilov morajo biti jasno in nedvoumno označene in postavljene tako, da so dostopna jih je mogoče uporabiti v primeru izrednih razmer.

Kadar je le mogoče, morajo biti kabli položeni podometno ali v zemlji. Kadar so položeni nadometno ali drugače izpostavljeni okolju in fizičnemu dostopu, morajo biti zaščiteni z ustreznim ohišjem oziroma zaščito.

Opreme, informacij in programske opreme ni dovoljeno iznašati iz poslovnih prostorov. Izjema so uporabniki, ki imajo pooblastilo za uporabo prenosnih naprav tudi zunaj poslovnih prostorov družbe.

V primeru iznosa opreme zaradi popravil ali drugih izrednih razlogov mora biti oprema, informacije ali programska oprema vodena v evidenci opreme, ki se nahaja zunaj prostorov. Oprema mora biti vrnjena v poslovne prostore najkasneje v dveh mesecih od iznosa.

Varno uničenje opreme in ravnanje z rabljenimi nosilci podatkov opredeljuje dokument DW P 05.

2.14 Politika čiste mize in praznega zaslona

Zaposleni morajo upoštevati načelo čiste mize. Ta določa, da ni dovoljeno puščati vsaj informacij in materialov z unikatnimi podatki ali unikatno funkcijo ter strateško zaupnih podatkov na mizi v času svoje odsotnosti, priporočeno pa je, da je miza v tem času prazna. Te materiale je potrebno hraniti v zaklenjenih predalih, omarah ali sobi. Informacije z unikatnimi podatki so informacije, ki omogočajo identifikacijo uporabnika, posameznika ali podjetja (predvsem uporabniška imena in gesla, pametne kartice, ključki za ustvarjanje enkratnih gesel ipd.), materiali z unikatnimi podatki so predvsem žigi in strateško zaupni podatki predvsem pogodbe, ponudbe, poročila in drugi dokumenti z zaupnimi podatki o cenah in stroških ter nosilci podatkov, ki vsebujejo večjo količino zaupnih informacij.

Pravila čiste mize in praznega zaslona so opredeljena v dokumentu DW P 02.

2.15 Varnost operacij

Operativni postopki morajo biti dokumentirani v obliki pisnih navodil ali podrobnih postopkov.

Spreminjanje nastavitev delovne postaje (npr. spreminjanje parametrov dostopa do interneta, izklapljanje protivirusne zaščite, požarne pregrade, ...) s strani uporabnika ali druge nepooblaščene osebe ni dovoljeno.

Vse spremembe informacijskega sistema morajo biti nadzorovane.

Vsaka sprememba mora biti vpisana v seznam sprememb, iz katerega je razvidno kdo in kdaj je podal nalogo za spremembo, kdo je spremembo izvedel in kdo potrdil ter kdaj je bila sprememba zaključena.

Za vsako spremembo mora biti obravnavan tudi varnostni vidik spremembe.

Pred potrditvijo spremembe mora lastnik vira preveriti pravilnost delovanja v testnem okolju ali na vsaj omejenem številu naprav.

Razen funkcionalnega testiranja mora biti izvedeno varnostno testiranje spremembe ali vsaj ocenjen vpliv na varnostno tveganje. Če je ocenjeni vpliv majhen, izvedba varnostnega testiranja ni obvezna.

Lastnik informacijskega sredstva je dolžan spremljati zmogljivosti svojega sredstva in načrtovati preostalo zmogljivost sredstva in predvideno izrabo zmogljivosti ter napovedati razširitev zmogljivosti sredstva ali zamenjavo sredstva z novim vsaj eno leto pred načrtovanim pomanjkanjem zmogljivosti sredstva.

Razvojno okolje mora biti dosegljivo razvijalcem in ne sme obdelovati osebnih podatkov.

Testno okolje sme vsebovati osebne in druge zaupne podatke samo v primeru, če uporablja enako kontrolo dostopa kot produkcijsko okolje in pooblašča za dostop le uporabnike, ki bi imeli dostop do teh podatkov tudi v produkcijskem okolju.

Razvijalci ne smejo imeti dostopa do produkcijskega okolja. Namestitve programske opreme, nastavitve in druge spremembe v produkcijskem okolju lahko izvaja le administrator produkcije na podlagi potrjenega zahtevka za namestitev.

2.16 Zaščita pred zlonamerno programsko opremo

Vse delovne postaje in strežniki morajo imeti nameščeno programsko opremo za protivirusno zaščito.

Protivirusna zaščita mora biti nastavljena tako, da se samodejno posodablja.

Uporabniki morajo biti ob rednem izobraževanju s področja informacijske varnosti informirani o pomembnosti protivirusne zaščite in osveščeni v zvezi z omejitvami samodejne zaščite.

Uporabnik mora spoštovati naslednje zahteve:

- ne sme namerno nameščati zlonamerne programske opreme v naprave ali je namerno širiti,
- v primeru suma zlonamerne programske opreme mora o tem takoj obvestiti odgovorno osebo za informacijsko varnost in postopati po njenih navodilih,
- ne sme odpirati in zaganjati njemu nepoznanih datotek, če ne pozna njihovega izvora,
- v primeru suma ali ugotovitve, da sistem protivirusne zaščite ne deluje ali ni ustrezno posodobljen, mora takoj obvestiti lastnika ali odgovorno osebo za informacijsko varnost,
- ne sme preusmerjati obvestil o morebitnih resničnih ali lažnih novih virusih drugim uporabnikom, prijateljem in znancem. O sumljivi elektronski pošti mora nemudoma poročati skrbniku ali informacijskemu varnostnemu inženirju.

Uporabnik v delovno postajo ne sme vstavljati nosilcev podatkov, ki niso njegovi. Če uporabnik najde nosilec podatkov ali ga prejme fizično od druge osebe, mora o tem nemudoma obvestiti skrbnika informacijske varnosti in upoštevati njegova navodila pri nadaljnji uporabi prenosnega nosilca podatkov.

Kadar je le mogoče, mora uporabnik pri prenosu podatkov na računalniške naprave izven informacijskega sistema družbe uporabiti nosilce podatkov, ki onemogočajo pisanje na nosilec podatkov (npr. zgoščenko, USB ključ s fizičnim stikalom za preprečevanje pisanja) z namenom, da bi se izognil okužbi svojega nosilca podatkov pri uporabi v drugem informacijskem sistemu.

2.17 Varnostno kopiranje informacij

Varnostno kopiranje pomembnih poslovnih informacij mora biti samodejno in se mora izvajati vsaj enkrat dnevno.

Varnostno kopiranje mora biti arhitekturno zasnovano tako, da škodljiva programska koda ne more hkrati z delovno kopijo podatkov šifrirati, izbrisati ali drugače poškodovati ali narediti nedostopnih tudi varnostnih kopij podatkov.

Obstajati mora varnostna kopija pomembnih informacij vsaj za prejšnji dan.

2.18 Beleženje dogodkov

Operacijski sistemi delovnih postaj morajo beležiti vsaj prijavo in odjavo uporabnikov.

Dnevnik beleženja na delovnih postajah mora beležiti dogodke vsaj za zadnji teden.

Dnevnik beleženja na strežnikih mora beležiti dogodke vsaj za zadnje tri mesece.

Vključeno mora biti beleženje ključnih opravil privilegiranih uporabniških računov (administratorjev).

Beleženi dogodki se štejejo kot pomembna poslovna informacija, zato mora biti zanje izdelana varnostna kopija podatkov.

Samo privilegirani uporabniški računi (administratorji) lahko imajo pooblastilo za spreminjanje nastavitev in brisanje dogodkov.

Ure naprav, ki beležijo čas, morajo biti usklajene z zunanjim časovnim strežnikom in se morajo usklajevati samodejno.

2.19 Nadzor operativne programske opreme

Odgovorna oseba za informacijsko varnost mora redno, vsaj enkrat mesečno spremljati ranljivosti, povezane z opremo, ki je v podjetju v uporabi.

Odgovorna oseba za informacijsko varnost sprejme odločitev o nujnosti namestitve varnostnih popravkov in za namestitev popravkov odpre zahtevo za spremembo.

Za vso opremo, ki podpira samodejno posodabljanje, mora biti samodejno posodabljanje vključeno.

Uporabniki ne smejo sami nameščati programske opreme. Vsa programska oprema mora biti nameščena skladno s procesom upravljanja sprememb.

2.20 Upoštevanje presoj informacijskih sistemov

Presojo varnosti informacijskega sistema je treba izvesti vsaj enkrat letno in ob večjih spremembah informacijskega sistema, ki vpliva na prepoznana tveganja.

Presoje ne smejo vplivati na operativno delovanje informacijskega sistema in na produkcijske sisteme.

2.21 Upravljanje varovanja omrežij

Ob priklopu v lokalno računalniško omrežje družbe je potrebno upoštevati naslednje zahteve:

- v omrežju se ni dovoljeno predstavljati kot nekdo drug (maskiranje),
- prisluškovanje omrežnemu prometu ni dovoljeno,
- poganjanje sistemskih in varnostnih aplikacij na sistemih ni dovoljeno, razen pooblaščenim osebam,
- dodajanje mrežnih naprav, ki razširjajo infrastrukturo družbe (stikalo, usmerjevalnik, razdelilnik, modem, brezžična dostopna točka ipd.) ni dovoljeno, razen pooblaščenim osebam,
- uporabnik, ki dodaja mrežne naprave v omrežje družbe, je odgovoren za njihovo uporabo in prav tako za dejavnosti vseh uporabnikov, ki so priključeni na to napravo.

Priklop sistemov ali omrežij na druge sisteme ali omrežja, vključno z internetom, ali direktne povezave, predstavlja za družbo varnostno grožnjo, zato veljajo naslednje zahteve:

- dostop do drugih omrežij je dovoljen le na sistemsko odobren način, ni dovoljen mimo varnostnih mehanizmov zaščite družbe,
- pred priključitvijo v informacijske sisteme ali omrežje družbe iz zunanjih omrežij mora biti uporabnik registriran in mora uporabiti dovoljene vhodne točke. Dostop se uredi na pisno zahtevo in ob odobritvi odgovorne osebe.

Povezava z internetom mora biti od internega omrežja ločena s požarnim zidom.

Požarni zid ne sme prepuščati prometa iz zunanjega v notranje omrežje, razen za dokumentirane storitve, nameščene v notranjem omrežju, za katere je bil dostop omogočen skladno s postopkom upravljanja sprememb.

Usmerjanje omrežnega prometa mora biti nastavljeno tako, da daje prednost podatkom, ki prenašajo videokonferenčne podatke.

Če so v internem omrežju nameščene storitve, ki so dostopne zunanjim uporabnikom, morajo biti te storitve nameščene v ločenem omrežju, ki nima neposrednega dostopa do uporabniškega dela omrežja.

Zaposleni lahko dostopajo do informacijskih virov na daljavo z uporabo splošno dostopnih komunikacijskih poti in uporabi šifrirane povezave do omrežja družbe.

Uporabniki, ki iz zunanjih omrežij dostopajo v notranje omrežje, morajo uporabljati šifrirano VPN povezavo.

Pri delu na daljavo, kjer ne uporabljamo informacijskih sredstev v lasti družbe in za katere ne skrbi družba, je potrebno upoštevati:

- na informacijsko napravo ne prenašamo informacijskih vsebin, ki so označene kot zaupne,
- če za oddaljen pristop uporabljamo spletni brskalnik, ga po končanem delu zapremo in pobrišemo vse delovne procese-aplikacije,
- vse delovne dokumente, ki smo jih ustvarili na oddaljenem informacijskem sredstvu izbrišemo in zapremo aplikacije.

Pred prenosom informacij med družbo in njenimi poslovnimi partnerji mora uporabnik, ki izmenjuje podatke s poslovnim partnerjem, pred izmenjavo informacij dogovoriti postopke za varno izmenjavo informacij in jih skladno z dogovorom uporabljati.

Kadar je s partnerji sklenjena pisna pogodba, mora ta vsebovati dogovor o zaupnosti in ne razkrivanju.

Pregled ustreznosti dogovorov o nerazkrivanju mora biti del rednega letnega pregleda varnostne politike in zunanjih izvajalcev.

2.22 Varnost v procesih razvoja in podpore

Specifikacije programske opreme morajo vsebovati tudi nefunkcionalne specifikacije in varnostne vidike zahtev.

Pri razvoju programske opreme mora biti upoštevana dobra praksa glede na platformo in vrsto storitve. Za spletne aplikacije mora biti pri razvoju upoštevan vsakokratno veljaven seznam »OWASP Top 10«.

2.23 Upravljanje varnostnih incidentov

Vsak uporabnik informacijskega sistema je dolžan vsak dogodek, ki lahko vpliva na varnost informacij, sporočiti odgovorni osebi za informacijsko varnost, ki ugotovi ali dogodek predstavlja varnostni incident.

V primeru neobičajnega obnašanja informacijskega sistema je uporabnik dolžan obvestiti odgovorno osebo za informacijsko varnost in ravnati po njenih navodilih. Družba vodi evidenco informacijskih incidentov, ki jo redno pregleduje odgovorna oseba za informacijsko varnost in izvaja ustrezne varnostne ukrepe.

Ob sumu, da se dogaja ali se je zgodil informacijski varnostni incident, je potrebno takoj, najkasneje pa v 24 urah, obvestiti odgovorno osebo za informacijsko varnost po telefonu in se ravnati po posredovanih navodilih.

Po telefonski prijavi incidenta je dolžan prijavitelj odgovorni osebi za informacijsko varnost naknadno posredovati tudi pisno prijavo.

V primeru suma varnostnega incidenta priključene naprave, mora uporabnik najprej izključiti napravo iz omrežja, če to ni mogoče pa izključiti električno napajanje, kar vključuje tudi odstranitev baterije iz prenosne naprave.

Zaposleni ne smejo raziskovati ali izvajati akcije proti napadalcu/krivcu. Za obravnavo informacijskih varnostnih incidentov je zadolžena odgovorna oseba za informacijsko varnost.

Izguba elektronske naprave (npr. telefon, tablica, kartica zaposlenega, daljinec za alarmno napravo) ali nosilca podatkov (npr. zgoščenka, USB ključek) je varnostni incident.

Odgovorna oseba za informacijsko varnost mora voditi seznam varnostnih incidentov.

Letna analiza seznama varnostnih incidentov je podlaga za izboljšave sistema varovanja informacij in je del letnega poročila s področja informacijske varnosti.

Odgovorna oseba za informacijsko varnost ob prejemu informacije o varnostnem incidentu tega klasificira in ukrepa glede na naravo varnostnega incidenta.

Reševanje incidentov ima prednost pred upravljanjem problemov in upravljanjem sprememb.

Odgovorna oseba za informacijsko varnost ob prejemu varnostnega incidenta, za katerega je treba poročati o kršitvi kateremukoli nadzornemu organu, nemudoma poroča neposredno vodstvu družbe.

2.24 Neprekinjena informacijska varnost

Družba še nima načrta zagotavljanja neprekinjenega poslovanja ali neprekinjenega delovanja informacijskega sistema.

Pri vpeljavi neprekinjenega poslovanja ali neprekinjenega delovanja informacijskega sistema morajo nove rešitve upoštevati tudi zagotavljanje neprekinjene varnosti informacijskega sistema.

Do vzpostavitve neprekinjenega poslovanja ali neprekinjenega delovanja informacijskega sistema ostajajo postopki varovanja informacijskega sistema v primeru izrednih razmer enaki kot v običajnih razmerah.

2.25 Razpoložljivost naprav za obdelavo informacij

Na trenutni stopnji razvoja informacijskega sistema je kot začasne naprave za nadaljevanje dela mogoče uporabiti trenutno proste delovne postaje ali s sprostitvijo najmanj obremenjene delovne postaje.

V primeru, da bi iz analize tveganja sledilo, da so se povečala tveganja s področja zagotavljanja razpoložljivosti naprav za obdelavo informacij, je treba ustrezno posodobiti to varnostno politiko.

2.26 Uporaba elektronske pošte

Uporaba zasebnih elektronskih predalov je dovoljena. Uporabniki lahko uporabljajo spletne vmesnike elektronske pošte, do katerih je dostop tehnično omogočen in ki zasebnih sporočil in drugih vsebin ne shranjujejo na računalniški informacijski opremi družbe.

Veljajo tudi naslednja pravila:

- Elektronski naslovi za fizično osebo morajo biti oblike ime@realtronik.com Ime je lahko tudi krajše kot uradno ime in je lahko tako, kot ga oseba uporablja (Nikolaj – Niko, Aleksander - Sašo).
- Anonimni elektronski naslovi niso dovoljeni, izjema so splošni elektronski naslovi (npr. »info«, »podpora«).
- Dodeljen elektronski predal se uporablja za uradno komunikacijo z drugimi zaposlenimi ter partnerji in strankami družbe. Uporaba drugih elektronskih predalov uporabnika za komunikacijo v imenu družbe je prepovedana.
- Uporaba službenih elektronskih predalov za zasebna sporočila in shranjevanje ali prenos osebnih podatkov je prepovedana. Če uporabnik prejme sporočilo, ki predstavlja njegove osebne podatke ali osebno komunikacijo, ga mora nemudoma izbrisati. Za izmenjavo osebnih sporočil so namenjeni zasebni elektronski predali izven neposrednega nadzora družbe.
- Skrbnik sistema elektronske pošte ustvarja in ureja uporabniške poštne predale na zahtevo pristojnih oseb, ki mu posredujejo vse potrebne podatke.
- V primeru prenehanja uporabe ali ukinitve uporabniškega predala se ukine e-poštni naslov. Vsebina predala se lahko ohrani, ker službeni predali ne smejo vsebovati osebnih sporočil in podatkov.

- Preusmeritev elektronskih sporočil uporabnika v predal izven informacijskega sistema družbe iz razlogov zagotavljanja razpoložljivosti in varnosti ni dovoljena.
- Samodejna preusmeritev elektronske pošte uporabnika na drug elektronski naslov ni dovoljena. Namesto preusmeritve se uporablja samodejni odzivnik, ki pošiljatelja napoti na novi ustrezen elektronski naslov.
- Uporabnik ne sme preusmerjati elektronskih sporočil.
- Uporabnik ne sme uporabljati predala v neslužbene namene kot so pridobitna dejavnost, neslužbene (ankete in vprašalniki, trgovina, ipd.) in politične aktivnosti.
- Prepovedano je razpošiljanje vseh vrst neželene pošte.

Elektronska sporočila naj bodo kratka z malo priponk. Velikost poslane ali sprejete elektronske pošte skupaj s priponkami je omejena. V primeru, da je omejitev presežena, se sporočilo avtomatično zavrne. Pošiljatelj dobi obvestilo o zavrnitvi. Omejitev je preventivni ukrep za preprečevanje prekomernega obremenjevanja sistema.

Če uporabnik po pomoti prejme sporočilo, ki mu ni namenjeno, vsebine tega sporočila ne sme shraniti ali uporabljati za katerikoli namen. O pomoti je dolžan nemudoma obvestiti pošiljatelja in prejeto sporočilo takoj izbrisati.

Pri pošiljanju elektronskih sporočil mora uporabnik upoštevati načelo racionalnosti in varnosti.

Obsežnih priponk ne pošiljamo. Kadar je to nujno potrebno, jih pretvorimo v ustrezni format, ki omogoča tiskanje vsebine.

Iz varnostnih razlogov dokumentov s končnicami, ki omogočajo avtomatsko izvajanje, ni priporočljivo prenašati z elektronsko pošto. Zelo verjetno je, da bo prejemni poštni strežnik sporočilo s takšno priponko izbrisal.

Uporabnik se ne sme prijavljati s službenim naslovom na elektronske poštne sezname, če ti niso vsebinsko povezani z delovnimi nalogami uporabnika ali uporabljati službeni naslov elektronske pošte kot podatek pri izpolnjevanju elektronskih obrazcev, če ti niso vsebinsko povezani z delovnimi nalogami uporabnika.

Uporabnik mora vzdrževati svoj elektronski poštni predal tako, da po potrebi, ki jo narekujejo omejitve kapacitete ali druge omejitve, arhivira in izbriše vsa elektronska sporočila, ki jih ne potrebuje več v službene namene, sporočila zasebne narave pa sproti izbriše.

Skrbnik se lahko odloči za ukrepanje v primeru, če bi uporabnik:

- uporabljal elektronsko pošto za pošiljanje verižnih pisem,
- uporabljal elektronsko pošto za prenos množičnih sporočil (neželene pošte).

V primeru nedovoljene uporabe sistema za elektronska sporočila, lahko skrbnik uporabniku začasno onemogoči uporabo informacijskega sistema.