Različica: 2.0
Datum: 20. 4. 2022
Število strani: 4
Potrdil: Boštjan Kežmah
JAVNO

Politika informacijske varnosti

Vsebina

1. Uvod

Varnost upravljanja ključnih poslovnih informacij je bistvenega pomena za izvajanje vseh poslovnih procesov v družbi CEPRIS.

Podjetje s številnimi mehanizmi nadzoruje in upravlja strukturo odgovornosti in s postopki zagotavlja, da je varnost informacij sestavni del vseh njegovih poslovnih procesov, poslovanja in upravljanja.

Namen tega dokumenta je določiti politiko sistema upravljanja varnosti informacij podjetja in njegovih procesov. Področje uporabe je podrobno opredeljeno v dokumentu **Odločba o obsegu in mejah za potrebe ISO 27001** (v nadaljnjem besedilu ISMS, angl. Information Security Management System), in se nanaša na vse dejavnosti, ki so vključene v načrtovanje, namestitev in vzdrževanje kot tudi v razvoj in izdelavo varnostnih sistemov in avdio/video sistema. Razlogi za izbiro tega obsega za izvajanje ISMS so naslednji:

- družba v okviru svoje osnovne dejavnosti poseduje zaupne podatke o strankah, ki jih je dolžan varovati,
- družba je dolžna pravilno hraniti podatke o izvedenih zaščitnih sistemih,
- notranjost razvitega znanja in metod dela,
- komercialne informacije o odnosih s kupci in prodajalci so zaupne.

Vsaka kršitev zaupnosti, razpoložljivosti ali celovitosti ključnih informacij lahko povzroči pomemben vpliv na poslovanje družbe.

2. Politika ISMS

Odločitev vodstva podjetja je vzpostaviti, izvajati, nadzirati, preverjati, vzdrževati in izboljševati sistem upravljanja informacijske varnosti, da se na ustrezen način in v skladu z najvišjimi mednarodnimi standardi obvladuje tveganje informacijske varnosti podjetja.

Z vzpostavitvijo ISMS podjetje strankam in partnerjem zagotavlja dodatno zagotovilo o varnosti njihovih informacij in varnosti poslovnega sodelovanja, pri čemer upošteva ustrezne poslovne, pravne in pogodbene varnostne obveznosti.

Politika ISMS kaže odločenost in pripravljenost vodstva zaščititi vsa informacijska sredstva v smislu njegove celovitosti, zaupnosti in razpoložljivosti ter pravnih in poslovnih interesov podjetja.

Cilji informacijske varnosti na področju ISMS so: ohranjanje tveganja informacijske varnosti na sprejemljivi ravni, učinkovito upravljanje informacijske varnosti, vzpostavitev in vzdrževanje učinkovitega sistema pristojnosti in odgovornosti informacijske varnosti ter izpolnjevanje pogodbenih, pravnih in regulativnih varnostnih ter zakonskih obveznosti.

Učinkovitost sistemov upravljanja informacijske varnosti in izvedenega varnostnega nadzora za zaščito informacijskih sredstev se bo nenehno ocenjevala v skladu s kontekstom upravljanja s tveganji, ki je opredeljen v poslovniku in sistemu ISO 9001:2015.

Izvajanje potrebnih varnostnih kontrol se bo izvajalo na podlagi ocene in upravljanja tveganj varnosti informacij. Varnostni nadzor se bo uporabljal le, če je upravičen, funkcionalen, stroškovno upravičen in učinkovit.

Vodstvo podjetja bo zagotavljalo dovolj sredstev za izvajanje (vzpostavitev, izvajanje, nadziranje, spremljanje, preverjanje, vzdrževanje in izboljšanje) vseh potrebnih organizacijskih, postopkovnih in tehničnih varnostnih ukrepov.

Vsi zaposleni, tretje osebe, pravne ali fizične osebe, ki sodelujejo v poslovnih procesih podjetja, morajo upoštevati to politiko, vse nadaljnje politike in postopke, tehnične in organizacijske varnostne ukrepe ter vse poslovne, pravne in regulativne zahteve glede informacijske varnosti, opredeljene v področju uporabe ISMS.

Zaposleni in tretje osebe, ki na kakršen koli način sodelujejo pri poslovnih procesih družbe se redno seznanjajo z vsemi varnostnimi politikami in postopki, ki veljajo zanje. Na ta način prevzemajo tudi odgovornost za informacijsko varnost, v primeru kršitve varnostnih politik in postopkov pa so odgovorni v skladu s pogodbenimi obveznostmi in internimi akti družbe.

Redno spremljanje izvajanja politike sistema upravljanja informacijske varnosti se bo izvajalo z dejavnostmi notranje revizije ISMS in preverjanjem učinkovitosti izvedenih varnostnih kontrol.

3. Struktura odgovornosti za informacijsko varnost

Vodstvo družbe je odgovorno za:

- vzpostavitev in vzdrževanje politike ISMS in ciljev informacijske varnosti v okviru ISMS,
- določitev obsega ISMS,
- zagotavljanje, da zaposleni v vseh potrebnih oddelkih sodelujejo pri zagotavljanju učinkovitega izvajanja ukrepov za varnost informacij na vseh področjih v okviru ISMS,
- imenovanje predstavnika, pristojnega za področje ISMS,
- imenovanje vodje informacijske varnosti na področju ISMS,
- imenovanje/izbiro notranjega ocenjevalca ISMS.

Predstavnik upravljanja ISMS je pooblaščen in odgovoren za:

- zagotavljanje zadostnih virov za vzpostavitev, izvajanje, spremljanje, preverjanje, vzdrževanje in izboljšanje ISMS,

- zagotavljanje virov za nadaljnje izvajanje programa usposabljanja in ozaveščenosti o varnosti informacij za zaposlene v ISMS za zmanjšanje tveganj v zvezi z varnostjo informacij in učinkovito obvladovanje incidentov na področju varnosti,
- odločanje o merilih za sprejemanje tveganja in sprejemljive stopnje tveganja za informacijsko varnost v okviru ISMS,
- zagotavljanje, da se notranje revizije ISMS redno izvajajo,
- po potrebi v primeru varnostnega incidenta kontaktira in usklajuje postopke s pristojnimi organi.

Upravljavci na svojem območju odgovornosti so pooblaščeni in odgovorni za:

- dodelitev funkcij in odgovornosti za varnost informacij zaposlenih,
- opredelitev poslovnih, pravnih in pogodbenih varnostnih zahtev,
- upravljanje sprememb informacijskih sredstev v skladu s poslovnimi, pravnimi in varnostnimi zahtevami,
- določitev pravice do dostopa do informacijskih sredstev ter izvajanje in preverjanje postopka razvrščanja informacijskih sredstev,
- dodelitev odgovornosti za izvajanje dejavnosti, opredeljenih v načrtu za obvladovanje tveganja ,
- odobritev dokumentov, potrebnih za učinkovito upravljanje informacijske varnosti,
- po potrebi v primeru varnostnega incidenta kontaktira in usklajuje postopke s pristojnimi organi.

Vodja varnosti informacij je pooblaščen in odgovoren za:

- začetek in usklajevanje izvajanja ocene tveganja in upravljanja informacijske varnosti,
- uskladitev izvajanja varnostnih ukrepov na vseh ravneh in o njihovi učinkovitosti poročati poslovodstvu in upravljavcem,
- zagotavljanje jasnega upravljanja in podpore vodstva za pobude za informacijsko varnost,
- zagon načrtov in programov za ohranjanje ozaveščenosti o varnosti informacij,
- vzdrževanje in izboljšanje metodologij in procesov upravljanja informacijske varnosti,
- usklajevanje izvajanja dejavnosti, opredeljenih v načrtu za obvladovanje tveganja,
- usklajevanje dejavnosti upravljanja kontinuitete poslovanja z vidika informacijske varnosti,
- prepoznavanje in poročanje o incidentih, ranljivosti in grožnjah, ki niso bili ustrezno obravnavani v dejavnostih upravljanja tveganj,
- poročanje o učinkovitosti ISMS in dajanje priporočil za izboljšanje,
- po potrebi v primeru varnostnega incidenta kontaktira in usklajuje postopke s pristojnimi organi.

Notranji presojevalec sistema upravljanja varovanja informacij je pristojen in odgovoren za izvajanje notranje revizije sistema in poročanje vodstvu družbe in lastnikom procesov. Vsi zaposleni so odgovorni za doseganje ciljev informacijske varnosti na svojem področju dela.

4. Ocena in obvladovanje tveganja informacijske varnosti

Ocena tveganja informacijske varnosti se izvaja v skladu z metodologijo, opisano v dokumentu z oceno tveganja.

Kriterij sprejemljivosti je opredeljen v dokumentu z oceno tveganja.

Glede na rezultate ocene tveganja bo opredeljen načrt obdelave tveganj, ki bo določil vse dejavnosti in odgovornosti za upravljanje nesprejemljivih tveganj informacijske varnosti, ki jim je podjetje izpostavljeno.

S podpisom načrta upravljanja tveganj je vodstvo pooblaščeno za izvajanje izbranih varnostnih kontrol in izvajanje ISMS.

5. Vzdrževanje, preverjanje in posodabljanje pravil ISMS in dokumentov o varnosti sistema

Odgovornost upravljavca informacijske varnosti je, da vsaj enkrat na leto pregleda in posodobi pravilnike ISMS ter vse dokumente, ki opredeljujejo politiko, procese ISO 9001:2015 in procese ISMS, ki dokumente pregleda, če je potrebno.

Vodja informacijske varnosti bo zagotovil razpoložljivost tega in vseh povezanih dokumentov ter zagotovil, da so varnostna politika, vsi standardi, smernice, operativni načrti in postopki, povezani s sistemom upravljanja informacijske varnosti, povezani tudi v sistem ISO 9001:2015 ter so razumljivi vsem zaposlenim in tretjim osebam.

6. Ukrepi

Vsako kršitev vsebine te politike, zakonov, splošnih aktov in vseh dokumentov, ki urejajo politiko, odgovornosti, procese in postopke v sistemu upravljanja informacijske varnosti družbe bo sankcionirano v skladu z zakonskimi predpisi in internimi akti podjetja. Nobene izjeme od tega pravilnika niso dovoljene.

7. Povezave

- Standard ISO 27001: 2005
- Standard ISO 27002: 2005
- Načrt za predelavo tveganj v okviru ISO 9001:2015
- Program usposabljanja in ozaveščanja o varnosti informacij
- Notranji postopek presoje ISMS
- Odločitev o imenovanjih v sistemu upravljanja informacijske varnosti
- Odločba o obsegu in mejah za potrebe ISO 27001