DATAINFO.SI, d.o.o.
Tržaška cesta 85, 2000 Maribor
www.datainfo.si I info@datainfo.si

Politika informacijske varnosti

Vsebina

1. Uvod

Varnost upravljanja ključnih poslovnih informacij je bistvenega pomena za izvajanje vseh poslovnih procesov v podjetju DATAINFO.SI d.o.o.

Podjetje s številnimi mehanizmi nadzora in upravlja strukturo odgovornosti in postopkov 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. Podroben področje uporabe opredeljeno v dokumentu Obseg sistema za upravljanje informacijske varnosti (v nadaljnjem besedilu *SUVI Eng. Information Security* management sistem), in se nanaša na vse dejavnosti, ki so vključeni v načrtovanje, namestitev in vzdrževanje, kot tudi razvoj in izdelavo varnostnih sistemov in avdio / video sistem . Razlogi za izbiro tega obsega za izvajanje SUVI so naslednji:

- DATAINFO.SI d.o.o. v okviru svoje osnovne dejavnosti poseduje zaupne podatke o strankah, ki jih

  je dolžan varovati.
- Podjetje DATAINFO.SI d.o.o je dolžno pravilno hraniti podatke o izvedenih zaščitnih sistemih.
- Notranjost razvitega znanja in metod dela je za vrednost vodnjaka T zelo pomembna .
- Komercialne informacije o odnosih s kupci in prodajalci so zaupne

DATAINFO.SI, d.o.o.
Tržaška cesta 85, 2000 Maribor
www.datainfo.si I info@datainfo.si

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

2. Politika SUVI

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

Cilji informacijske varnosti na področju SUVI 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 27001:2005.

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 (izvajanje, izvajanje, 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 področje uporabe SUVI.

Zaposleni in tretje osebe, na kakršen koli način, ki sodeluje pri poslovnih procesih podjetja DATAINFO.SI d.o.o., 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 podjetja DATAINFO.SI d.o.o..

DATAINFO.SI, d.o.o.
Tržaška cesta 85, 2000 Maribor
www.datainfo.si I info@datainfo.si

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

3. Struktura odgovornosti za informacijsko varnost

Vodstvo podjetja DATAINFO.SI d.o.o. je odgovorno za:

- Vzpostaviti in vzdrževati politike SUVI in cilje informacijske varnosti v okviru SUVI,
- Določitev obsega SUVI,
- Zagotavljanje, da zaposleni v vseh potrebnih oddelkih sodelujejo pri zagotavljanju učinkovitega izvajanja ukrepov za varnost informacij na vseh področjih v okviru SUVI,
- Imenovanje predstavnika , pristojnega za področje SUVI,
- Imenovanje vodje informacijske varnosti na področju SUVI,
- Imenovanje notranjega ocenjevalca SUVI.

Predstavnik upravljanja SUVI je pooblaščen in odgovoren za:

- Zagotavljanje zadostnih virov za vzpostavitev, izvajanje, izvajanje, spremljanje, preverjanje, vzdrževanje in izboljšanje SUVI,
- Zagotavljanje virov za nadaljnje izvajanje programa usposabljanja in ozaveščenosti o varnosti informacij za zaposlene v SUVI 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 SUVI,
- Zagotavljanje, da se notranje revizije SUVI redno izvajajo
- Po potrebi v primeru varnostnega incidenta kontaktirajte in usklajujte 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,

DATAINFO.SI, d.o.o.
Tržaška cesta 85, 2000 Maribor
www.datainfo.si I info@datainfo.si

- 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,

Vodja varnosti informacij je pooblaščen in odgovoren za:

- Začetek in usklajevanje izvajanja ocene tveganja in upravljanja informacijske varnosti,
- Uskladiti izvajanje varnostnih ukrepov na vseh ravneh in o njihovi učinkovitosti poročati poslovodstvu in upravljavcem,
- Zagotavljanje jasnega upravljanja in podpore uprave 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,
- Prepoznati in poročati o incidentih, ranljivosti in grožnjah, ki niso bili ustrezno obravnavani v dejavnostih upravljanja tveganj,
- Poročanje o učinkovitosti SUVI in dajanje priporočil za izboljšanje.

Notranji presojevalec sistem upravljanja varovanja informacij je pristojen in odgovoren za izvajanje notranje revizije sistema in poročanje vodstvu podjetja DATAINFO.SI d.o.o. in lastnikom procesov. Rezultati in postopek je natančneje opredeljen v poglavju Interne presoje. 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 Metodologija ocene informacijske varnosti .

Kriterij sprejemljivosti je opredeljen v Metodologiji za oceno tveganja za informacijsko varnost .

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.

DATAINFO.SI, d.o.o.
Tržaška cesta 85, 2000 Maribor
www.datainfo.si I info@datainfo.si

S podpisom načrta upravljanja tveganj je uprava pooblaščena za izvajanje izbranih varnostnih kontrol in izvajanje SUVI.

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

Odgovornost upravljavca informacijske varnosti je, da vsaj enkrat na leto pregleda in posodobi pravilnike SUVI ter vse dokumente, ki opredeljujejo politiko, procese ISO 27001:2005 in procese SUVI, 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 27001:2005, 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 podjetja DATAINFO.SI d.o.o., 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
- Ocena tvegan po procesih
- Program usposabljanja in ozaveščanja o varnosti informacij