**Ocena tveganja za poslovni proces Obravnavanje pacientov**



***»eZdravje«***

***OCENA TVEGANJA ZA POSLOVNI PROCES OBRAVNAVANJE PACIENTOV***

Status: OSNUTEK, Različica 0.1

Ljubljana, 08. 12. 2010



|  |  |  |  |
| --- | --- | --- | --- |
| Namen dokumenta: | | Ocena tveganj za poslovni proces Obravnavanje pacientov | |
| Vsebina | | Glej kazalo | |
| Oznaka dokumenta: | | <SVVI za izvajalce zdravstvene dejavnosti>-< >-<Končna> <1.0> | |
| Status: | | <Odobreno> | |
| Verzija: | | Končna 1.0 | |
| Datum kreiranja: | | Glej tabelo Zgodovina verzij | |
| Datum verzije: | | Glej tabelo Zgodovina verzij | |
| Naročnik/Uporabnik: | |  | |
| Avtorji: | |  | |
|  | |
| Zgodovina verzij: | |  | |
| **Verzija** | **Datum zadnje spremembe** | | **Opombe** |
| Osnutek 0.1 |  | |  |
| Osnutek 0.2 |  | |  |
| Končna 1.0 |  | |  |
| Stopnja zaupnosti: | | SAMO ZA INTERNO RABO | |

Kazalo vsebine

[1 OCENA TVEGANJA 5](#_Toc272406184)

[1.1 Zahteve procesa glede varovanja informacij 5](#_Toc272406185)

[1.2 Sklopi groženj in ocenjena tveganja 5](#_Toc272406186)

# OCENA TVEGANJA

## Zahteve procesa glede varovanja informacij

**Kritičnost poslovne aktivnosti:** visoka

**Aplikacije za podporo poslovne aktivnosti:** ISOZ

**Zaupnost informacij:** občutljivi osebni podatki

**Integriteta informacij:** visoka

**Toleriran čas izpada:** 1 ura

**Alternativni postopki:** (možno je ročno izvajanje aktivnosti brez podpore IT)

## Sklopi groženj in ocenjena tveganja

Pri ocenjevanju verjetnosti grožnje, stopnje posledic grožnje, stopnje ranljivosti in učinkovitosti protiukrepov je potrebno upoštevati navodila iz Postopka izvajanja analize tveganj.

1. **Okoljski vplivi**

**Grožnja: 1.1. Naravna nesreča-Potres**

Verjetnost grožnje: majhna*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izguba občutljivih osebnih podatkov*

Stopnja ranljivosti: nizka*(nizka, srednja ali visoka)*

*Komentar: ni potresno področje*

Učinkovitost protiukrepov: visoka *(nična, nizka, srednja ali visoka)*

*Komentar: protipotresna gradnja*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 1.2. Naravna nesreča-Ogenj**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke*(majhna, srednja ali visoka)*

*Komentar: : izguba občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja*(nizka, srednja ali visoka)*

*Komentar: človeški faktor*

Učinkovitost protiukrepov:visoka*(nična, nizka, srednja ali visoka)*

*Komentar: senzorji dima povezani z varnostno službo, gasilni aparati*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 1.3. Naravna nesreča-Zalitje vode**

Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke*(majhna, srednja ali visoka)*

*Komentar: : izguba občutljivih osebnih podatkov*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar: ni poplavnem področju, relativno nova stavba*

Učinkovitost protiukrepov:srednja*(nična, nizka, srednja ali visoka)*

*Komentar: papirna dokumentacija je shranjena v 1. Nadstropju v kartotečnih omarah*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 1.4. Naravna nesreča-Vpliv temperature**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka*(majhna, srednja ali visoka)*

*Komentar: odpoved informacijske podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega ( 4 ure)*

Stopnja ranljivosti: visoka *(nizka, srednja ali visoka)*

*Komentar: ni senzorjev previsoke temperature*

Učinkovitost protiukrepov:srednja *(nična, nizka, srednja ali visoka)*

*Komentar: klimatska naprava, ki ni podvojena*

Ocena tveganja: **5*(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 1.4.1: Podvojiti klimatski sistem in namestiti senzorje za previsoko temperaturo s sistemom obveščanja. *(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 1.5. Naravna nesreča- strela**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijske podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega (4 ure)*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: poletne nevihte*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: strelovod*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Odpoved infrastrukture**

**Grožnja: 2.1. Odpoved/okvara sredstev IT**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijske podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega (1 ura)*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: pomanjkljivi nadzorni mehanizmi, človeška napaka, degradacija opreme*

Učinkovitost protiukrepov:nizka *(nična, nizka, srednja ali visoka)*

*Komentar: sistemi niso podvojeni, ni načrtov ponovne vzpostavitve delovanja*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 2.1.1: Izdelava načrta neprekinjenega poslovanja v primeru odpovedi ali okvare sredstev IT

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 2.2. Odpoved oskrbe z električno energijo**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijske podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega (1 ura)*

Stopnja ranljivosti: srednja*(nizka, srednja ali visoka)*

*Komentar:javno električno omrežje*

Učinkovitost protiukrepov:nizka *(nična, nizka, srednja ali visoka)*

*Komentar: uporaba UPS-a, ki ni dovolj zmogljiv*

Ocena tveganja: **5** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 2.2.1: Nabaviti zmogljivejši UPS in agregat. *(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 2.3. Nihanja/sunki/udari električne energije**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijske podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega (1 ura)*

Stopnja ranljivosti: srednja*(nizka, srednja ali visoka)*

*Komentar:javno električno omrežje*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: uporaba UPS-a*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 2.4. Nezadostna zmogljivost IT/komunikacijske opreme**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 2.5. Odpoved javnih komunikacij**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka*(majhna, srednja ali visoka)*

*Komentar: izpad delovanja kritičnega poslovnega procesa*

Stopnja ranljivosti: visoka *(nizka, srednja ali visoka)*

*Komentar: napaka dobavitelja, poškodba kabla zaradi človeške napake*

Učinkovitost protiukrepov:nizka *(nična, nizka, srednja ali visoka)*

*Komentar: samo en dobavitelj storitve interneta*

Ocena tveganja: **5** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 2.5.1: Pridobiti nadomestnega ponudnika internetnih storitev, tako da bo povezava do interneta potekala po fizično ločenih poteh*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

Mateja.stanta.gov.si

**Grožnja: 2.6. Odpoved/okvara komunikacijskih sistemov**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijska podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega časa (4 ure)*

Stopnja ranljivosti: srednja*(nizka, srednja ali visoka)*

*Komentar: človeška napaka, degradacija oprema*

Učinkovitost protiukrepov:srednja *(nična, nizka, srednja ali visoka)*

*Komentar: požarna pregrada je podvojena, vendar je potreben ročni preklop, možen ročni preklop uporabnikov na neuporabljena vrata stikal*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 2.6.1: Podvojiti mrežno opremo (požarno pregrado in stikala).

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Logični vdori od zunaj**

**Grožnja: 3.1. Škodljiva koda (virusi, trojanska koda,..)**

Verjetnost grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka*(majhna, srednja ali visoka)*

*Komentar: razkritja občutljivih osebnih podatkov*

Stopnja ranljivosti: visoka*(nizka, srednja ali visoka)*

*Komentar: ranljivost Windows operacijsksega sistema*

Učinkovitost protiukrepov:srednja*(nična, nizka, srednja ali visoka)*

*Komentar: protivirusna programska oprema na delovnih postajah, ni centralizirano upravljano, posodablja se redno, ni nadzora nad posodabljanjem, operacijski sistem se posodablja, vendar ni nadzora, zaposleni imajo pravice navadnega uporabnika*

Ocena tveganja: **5** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 3.1.1: *Centralno upravljanje protivirusne programske opreme.*

Ukrepi 3.1.2: *Centralno upravljanje nameščanja popravkov operacijskega sistema (npr.: WSUS).*

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 3.2. Vdori v notranje omrežje-iz interneta**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje zdravstvenih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: varnostni pregled ni bil izveden*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: strežniki in požarna pregrada so ustrezno vzdrževani, preverja se elektronska pošta, omejevanje prometa s požarno pregrado, zunanji vzdrževalec ima v pogodbi člen o nerazkrivanju informacij*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 3.3. Vdori v notranje omrežje-v brezžično omrežje**

Verjetnost grožnje: nizka *(majhna, srednja ali visoka)*

*Komentar: omejen domet brezžičnega omrežja*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:srednji *(nična, nizka, srednja ali visoka)*

*Komentar: geslo za dostop je ustrezno dolgo, brezžično omrežje je ločeno od lokalnega omrežja*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: *Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Fizični dostopi**

**Grožnja: 4.1. Namerno ali nenamerno poškodovanje opreme**

Verjetnost grožnje: srednja*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izpad informacijska podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega časa (4 ure)*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:visoka*(nična, nizka, srednja ali visoka)*

*Komentar: pomembni računalniški sistemi so nameščeni v strežniški sobi, ki je zaklenjena, dostop imajo pooblaščeni zaposleni. Po delovnem času se vrata v Upravo zaklepajo. Ponoči se zaklepa stavba in vklopi alarm.*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 4.2. Kraja prenosne opreme**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar: človeški faktor*

Stopnja posledic grožnje: nizka *(majhna, srednja ali visoka)*

*Komentar: na prenosno opremo se ne shranjuje osebnih, občutljivih osebnih ali podatkov za interno rabo*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: ni varnostne politike, navodil, ni nadzora*

Učinkovitost protiukrepov:nična *(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 4.2.1: Uvesti šifriranje diskov prenosnih računalnikov.*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 4.3. Kraja opreme**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar: človeški faktor*

Stopnja posledic grožnje: visoka*(majhna, srednja ali visoka)*

*Komentar: izpad informacijska podpore kritičnemu poslovnemu procesu za daljši čas od toleriranega časa (4 ure)*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: pomembni računalniški sistemi so nameščeni v strežniški sobi, ki je zaklenjena, dostop imajo pooblaščeni zaposleni. Po delovnem času se vrata v Upravo zaklepajo. Ponoči se zaklepa stavba in vklopi alarm. V Upravi so obiskovalci vedno pod nadzorom. Pacienti so pod nadzorom zdravstvenega osebja. Ordinacije se zaklepajo, ni pa slepe kljuke.*

Ocena tveganja: **1 *(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 4.4. Kraja podatkov/dokumentov**

Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: majhne*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: občutljivi osebni v elektronski obliki so shranjeni v informacijskem sistema ZZZS*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 4.5. Kraja papirnih dokumentov**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar: človeški faktor*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: vsa zdravniška dokumentacija je v papirni obliki, v ambulantah ni slepih kljuk*

Učinkovitost protiukrepov:visoka*(nična, nizka, srednja ali visoka)*

*Komentar: pravilnik, kartoteke so zaklenjene v kartotečnih omarah. Pisarne se zaklepajo. Zdravstveno osebje je ozaveščeno.*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Napake pri obdelavi**

**Grožnja: 5.1. Razkritje dokumentov/podatkov (med prenosom podatkov po komunikacijskih linijah ali na prenosnem računalniku pri oddaljenem dostopu)**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: ni nadzora nad pošiljanjem elektronske pošte, elektronska pošta se ne šifrira, pravilnik o postopkih in ukrepih o zavarovanju osebnih podatkov*

Učinkovitost protiukrepov:srednja *(nična, nizka, srednja ali visoka)*

*Komentar: prenos podatkov z aplikacijo ISOZ je šifriran, oddaljen dostop poteka preko VPN povezave*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 5.1: Redno izobraževanje in ozaveščanje zaposlenih o prepovedi pošiljanja občutljivih osebnih podatkov v nešifrirani obliki po elektronski pošti*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.2. Odpovedovanje nosilcev zapisov**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.3. Razkritje gesla**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti:visoka (*nizka, srednja ali visoka)*

*Komentar: zaposleni si posojajo gesla, zaposleni si gesla zapisujejo, ni politike glede izbire in menjave gesel*

Učinkovitost protiukrepov:nična *(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja: 5 ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 5.3.1: Izdelati in vpeljati politiko varnega ravnanja z gesli.

Ukrepi 5.3.2: Izobraževati in ozaveščati zaposlene glede upoštevanja varnostne politike ravnanja z gesli.

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.4. Poškodba vodov**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.5. Napake pri prenosu**

Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke*(majhna, srednja ali visoka)*

*Komentar: izgube celovitosti občutljivih osebnih podatkov*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar: nezanesljivost povezave, slabi stiki*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: TCP protokol zagotavlja zanesljiv prenos, šifriranje*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.6. Napaka pri vzdrževanju**

Verjetnost grožnje: srednja*(majhna, srednja ali visoka)*

*Komentar: človeški faktor*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: odpoved informacijske podpore kritičnemu poslovnemu procesu*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: popravki se ne testirajo, navodila ne obstajajo*

Učinkovitost protiukrepov: srednja *(nična, nizka, srednja ali visoka)*

*Komentar: možna vrnitev v prvotno stanje, zunanji izvajalec je strokovno usposobljen*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 5.6.1: Izdelati postopke uvajanja sprememb in vzdrževanja sistemov in programske opreme. *(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.7. Odpoved/okvara programske opreme**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 5.8. Napaka zaposlenih**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke *(majhna, srednja ali visoka)*

*Komentar: izguba celovitosti občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: človeški faktor*

Učinkovitost protiukrepov:srednja*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja: **4 *(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 5.8.1: Uvesti nadzor zaposlenih glede pravilnosti vnašanja občutljivih osbnih in osebnih podatkov.

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Napake in pomanjkanje nadzora pri razvoju in vzdrževanju**

**Grožnja: 6.1. Neustrezni zapisi o spremembah/popravkih**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.2. Priložnost za dostop preko stranskih vrat**

Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: visoka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov: visoka *(nična, nizka, srednja ali visoka)*

*Komentar: redno pregledovanja zapisov o dostop do spleta in skozi požarno pregrado.*

Ocena tveganja: **2** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.3. Celovito testiranje ni zagotovljeno**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.4. Frustracija uporabnikov**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.5. Težko odkrivanje napak**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.6. Slab nadzor metodologije kodiranja**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.7. Preverjanje oteženo/nemogoče**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: kršenje zakonodaje in pravilnika*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: konfiguracije strežnikov in programske opreme*

Učinkovitost protiukrepov: srednja *(nična, nizka, srednja ali visoka)*

*Komentar:revizijske sledi dostopa do občutljivih osebnih podatkov zagotavlja ISOZ. Administratorji se prijavljajo vsak s svojimi uporabniškim imenom. Beležijo se revizijske sledi na strežnikih, stikalih in požarni pregradi. Revizijske sledi se ne izvažajo na centralno mesto. Ni politike revizijskih sledi.*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: Namestitev strežnika za zbiranje revizijskih sledi in njihovo ustrezno shranjevanje. *(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 6.8. Nepričakovano delovanje**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Neizvajanje varnostnih predpisov**

**Grožnja: 7.1. Zloraba storitev elektronske pošte in dostopa do interneta**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov, izguba ugleda organizacije*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: ni politike uporabe spleta in elektronske pošte, internetnih strani se ne blokira*

Učinkovitost protiukrepov: srednja *(nična, nizka, srednja ali visoka)*

*Komentar: elektronska pošta se protivirusno preverja, omejena je velikost elektronskih sporočil,*

Ocena tveganja: **4** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 7.1.1.: Vpeljava politike uporabe spleta in elektronske pošte. *(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.2. Neuporaba programskih popravkov za odstranitev znanih varnostnih lukenj**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.3. Slabšanje papirne dokumentacije**

Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: izguba občutljivih osebnih podatkov*

Stopnja ranljivosti: *visoka* *(nizka, srednja ali visoka)*

*Komentar:* vsa dokumentacija je v papirni obliki

Učinkovitost protiukrepov:srednja *(nična, nizka, srednja ali visoka)*

*Komentar: arhiv je v zaklenjeni sobi na policah.*

Ocena tveganja: **3 *(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.4. Nenadzorovano ravnanje**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.5. Odpoved/nedosegljivost varnostne kopije podatkov**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.6. Kršenje zakonodaje**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke *(majhna, srednja ali visoka)*

*Komentar: kršenje zakonodaje*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: človeški faktor*

Učinkovitost protiukrepov:srednja*(nična, nizka, srednja ali visoka)*

*Komentar:* Pravilnik o postopkih in ukrepih za varovanje osebnih podatkov, interno izobraževanje

Ocena tveganja: 4 ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi7.6.1: Izdelati natančna navodila glede ravnanja z osebnimi in občutljivimi osebnimi podatki.

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 7.7. Kraja/izguba opreme/podatkov pri delu na daljavo**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Zloraba infrastrukture**

**Grožnja: 8.1. Zloraba skrbniških pravic**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.2. Socialni inženiring**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke*(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: človeški faktor*

Učinkovitost protiukrepov: nizka *(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja: **5** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 8.2.1: Redno ozaveščanje zaposlenih o nevarnostih socialnega inženiriringa.*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.3. Neustrezna uporaba nosilcev zapisa** (npr: shranjevanje zaupnih podatkov Verjetnost grožnje: majhna *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoke *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: nizka *(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:visoka *(nična, nizka, srednja ali visoka)*

*Komentar: podatkov iz aplikacije ISOZ ni možno izvoziti*

Ocena tveganja: **1** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.4. Dostop tretjih oseb do sistemov/dokumentov**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritja občutljivih osebnih podatkov*

Stopnja ranljivosti: srednja *(nizka, srednja ali visoka)*

*Komentar: V pogodbah s tretjimi strankami ni določila glede varovanja informacij.*

Učinkovitost protiukrepov:srednja *(nična, nizka, srednja ali visoka)*

*Komentar: Tretje osebe so vedno pod nadzorom nekoga od zaposlenih. Strežniška soba in ordinacije se zaklepajo. Čiščenje izvajajo zaposleni.*

Ocena tveganja: 4 ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi 8.4.1: Vse tretje stranke morajo podpisati sporazum o nerazkrivanju informacij.

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.5. Zloraba programske opreme** (npr.: nepooblaščen, neodobren, nezakonit način uporabe)

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.6. Zloraba omrežja (uporaba omrežja na neodobren način, priključitev neodobrene opreme, preusmeritev komunikacij, analiza prometa)**

Verjetnost grožnje: srednja *(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: visoka *(majhna, srednja ali visoka)*

*Komentar: razkritje občutljivih osebnih podatkov*

Stopnja ranljivosti: visoka *(nizka, srednja ali visoka)*

*Komentar: možnost priključitve neodobrene opreme, zunanji najemniki nimajo ustrezno omejenega dostopa do omrežja, možnost prestrezanja prometa,*

Učinkovitost protiukrepov:nizka*(nična, nizka, srednja ali visoka)*

*Komentar: v javnih prostorih in hodnikih ni vtičnic*

Ocena tveganja: **5** ***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrep 8.6.1: Zunanje najemnike se priključi v ločen segment omrežja.

*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

**Grožnja: 8.7. Zloraba uporabniških pravic**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*

1. **Nerazpoložljivost kadrov**

**Grožnja: 9.1. Smrt/poškodba zaposlenih**

Verjetnost grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja posledic grožnje: \_\_\_\_\_\_\_\_\_\_\_\_\_*(majhna, srednja ali visoka)*

*Komentar:*

Stopnja ranljivosti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(nizka, srednja ali visoka)*

*Komentar:*

Učinkovitost protiukrepov:\_\_\_\_\_\_\_\_\_\_\_\_\_*(nična, nizka, srednja ali visoka)*

*Komentar:*

Ocena tveganja:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(vrednost se odčita iz Tabel 1 in 2 v dokumentu Postopek izvajanja analize tveganja)***

Ukrepi: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Če je tveganje* ***višje od 3****, se predlaga ukrepe za znižanje tveganja.)*