PODROČNE POLITIKE VAROVANJA INFORMACIJ

IZDELALA	PREGLEDALA	ODOBRILA
E-žig ustvarjen za: Jan Sinigoj jan.sinigoj@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 06.08.2025 Potek veljavnosti potrdila: 04.04.2030 Jan Sinigoj	E-žig ustvarjen za: Oton Gortnar oton.gortnar@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 06.08.2025 Potek veljavnosti potrdila: 04.04.2030 mag. Oton Gortnar	E-žig ustvarjen za: Marjan Eberlinc marjan.eberlinc@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 07.08.2025 Potek veljavnosti potrdila: 04.04.2030 Marjan Eberlinc
E-žig ustvarjen za: Bojan Pečar bojan.pecar@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 06.08.2025 Potek veljavnosti potrdila: 04.04.2030 mag. Bojan Pečar	E-žig ustvarjen za: Tadej Tanko tadej.tanko@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 07.08.2025 Potek veljavnosti potrdila: 04.04.2030	E-žig ustvarjen za: Matija Bitenc Matija.Bitenc@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 11.08.2025 Potek veljavnosti potrdila: 04.04.2030 mag. itenc

Na osnovi določil točk Devetič in Dvanajstič Akta o ustanovitvi družbe z omejeno odgovornostjo PLINOVODI d.o.o., po posredovanju v mnenje Sindikatu delavcev družbe Plinovodi d.o.o. z dne 24. 6. 2025 ter na podlagi sklepa 34. seje Poslovodstva družbe PLINOVODI d.o.o. z dne 6. 8. 2025, sprejme Poslovodstvo družbe naslednje področne politike varovanja informacij:

Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami
Politika fizične zaščite in fizičnega dostopa
Politika nadzora dostopa do aplikacij, informacij in sistemov
Politika upravljanja in varovanja gesel
Politika varovanja v zvezi z osebjem
Politika revizijskih sledi
Politika zagotavljanja kakovosti infrastrukture
Politika varnostnega kopiranja
Politika izdelave in hrambe dokumentarnega in arhivskega gradiva
Politika razvoja, spreminjanja in vzdrževanja programske opreme
Politika nadzora sprememb informacijskega sistema
Politika zaščite pred zlonamerno programsko opremo
Politika upravljanja kakovosti in varnosti storitev tretjih strank
Politika upravljanja varnostnih incidentov

KAZALO

1 POLITIKA O NAVODILIH ZA KLASIFIKACIJO, OZNAČEVANJE IN RAVNANJE Z INFORMACIJAMI

1.1 Namen

Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami določa pravila in postopke klasifikacije podatkov ter odgovornosti pri njihovem upravljanju. Pravila in postopki zmanjšajo možnost nepooblaščene uporabe, ki ima lahko za posledico razkritje podatkov. Pravila klasifikacije morajo biti usklajena z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje dejavnosti. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki zadevajo zaščito dostopov do informacij in storitev. Politiko o navodilih za klasifikacijo, označevanje in ravnanje z informacijami je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

1.2 Lastništvo in informacije

Družba je lastnik vseh informacij, s katerimi v procesu upravlja. To so informacije, ki se uporabljajo za izvrševanje delovnih nalog. Lastniki informacij so odgovorni za določanje primerne stopnje klasifikacij informacij, ki so opredeljene kot:

- Tajni podatki

Tajne podatke predstavljajo podatki, ki lahko ob razkritju škodljivo vplivajo na družbo in Republiko Slovenijo. Tajne podatke opredeljuje Pravilnik o varovanju tajnih podatkov stopnje INTERNO.

- Osebni podatki

Osebni podatki (Zakon o varstvu osebnih podatkov) se uporabljajo pri izvajanju dejavnosti in se nanašajo na posameznika ne glede na obliko, v kateri so izraženi. Njihovo nepooblaščeno razkritje lahko resno škodi družbi in njihovim uporabnikom. Osebne podatke opredeljuje Pravilnik o določanju tajnosti poslovnih skrivnosti ter varstvu osebnih in poslovno občutljivih podatkov.

- Poslovna skrivnost in poslovno občutljivi podatki

Poslovno skrivnost predstavljajo podatki, ki lahko ob razkritju škodljivo vplivajo na družbo in njegove uporabnike. Poslovno skrivnost opredeljuje Pravilnik o določanju tajnosti poslovnih skrivnosti ter varstvu osebnih in poslovno občutljivih podatkov.

- Javno

Vsi podatki, za katere se dovoli, da se jih sme javno objaviti. Za take informacije tudi nepooblaščeno razkritje ne pomeni grožnje. Primeri takšnih informacij so objave v medijih.

1.3 Lastništvo in dovoljenje do dostopa

Lastniki morajo odločati o tem, kdo pridobi dovoljenje dostopa do informacij in na kakšen način se bo s to informacijo ravnalo glede na njeno klasifikacijo. Lastniki določijo, kako se bo izvajal primeren nadzor pri hranjenju, ravnanju, širjenju in drugi uporabi informacij.

1.4 Odgovornosti uporabnikov informacij

Vsi uporabniki informacijskega sistema, ki pridejo v stik z osebnimi podatki in poslovno skrivnostjo, morajo poznati politiko o navodilih za klasifikacijo, označevanje in ravnanje z informacijami ter jo učinkovito izvajati kot del vsakodnevnih nalog pri delu.

1.5 Označevanje informacij

Osebni podatki ter poslovna skrivnost lahko od nastanka do uničenja označujemo s primerno oznako klasifikacije informacij ali hranjeni tako, da je se ločijo od ostalih neklasificiranih podatkov. Uporabniki ne smejo odstranjevati ali spreminjati oznak klasifikacije informacij, razen če so za to prejeli dovoljenje lastnika.

1.6 Označevanje elektronskih izvodov informacij

Računalniške datoteke, ki vsebujejo osebne podatke ali poslovno skrivnost morajo imeti jasno oznako klasifikacije, ki je določena v metapodatkih datoteke oziroma biti hranjena skladno s klasifikacijsko shemo (označitev klasifikacije za posamezne informacijske sisteme).

2 POLITIKA FIZIČNE ZAŠČITE IN FIZIČNEGA DOSTOPA

2.1 Namen

Politika fizične zaščite in fizičnega dostopa določa pravila in postopke fizičnih dostopov do informacijskega sistema. Pravila in postopki omogočajo dostop do informacijskega sistema za pooblaščene osebe. Nepooblaščen dostop ima lahko za posledico razkritje podatkov, med katere spadajo osebni podatki in poslovna skrivnost. Pravila in postopki fizične zaščite in fizičnega dostopa morajo biti usklajeni z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje dejavnosti. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki zadevajo zaščito dostopov do informacij in storitev. Politiko fizične zaščite in fizičnega dostopa je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

2.2 Fizični dostop do varovanih območij

Varovanje posameznih prostorov se razlikuje po tem, v kakšno območje spadajo. Pri tem se ne sme ovirati izvajanja dejavnosti družbe. Objekti družbe so varovani na način, da je možen samo pooblaščen dostop oziroma se nadzira dostop do območja družbe.

- Območje javnega dostopa

Pred območjem družbe, kjer se izvaja varovanje, se lahko pojavlja območje javnega dostopa, ki ni posebej varovano, zato se v tem območju ne sme hraniti in obdelovati osebnih podatkov ali poslovnih skrivnosti. Te prostore se nadzoruje, da se obiskovalci nahajajo tam samo v delovnem času in za namene uporabe storitev, obiska oziroma zaradi pogodbenih obveznosti.

- Območje upravnih pisarn (pisarne oziroma prostori družbe, kjer se nahajajo podatki ali sredstva informacijskega sistema (delovne postaje, prenosniki ipd.))

Območje upravnih pisarn je namenjeno hrambi in obdelavi osebnih podatkov in poslovne skrivnosti ter zajemu dokumentarnega gradiva. Zagotavlja se primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ oziroma brezkontaktna kartica), tako da je dostop možen samo z izbranim sredstvom kontrole dostopa. Prostori, kjer se hranijo osebni podatki in poslovna skrivnost, so lahko izven delovnega časa nadzorovani z načini tehničnega varovanja (kontrola vstopnih točk s protivlomnim alarmom in varnostno službo).

- Območje računalniškega IS (podatkovni center itd., kjer se izvaja hramba dokumentarnega gradiva)

Območje računalniškega IS je namenjeno postavitvi ključnih, krmilnih in nadzornih informacijskih sistemov, hrambi in obdelavi osebnih podatkov in poslovne skrivnosti ter hrambi dokumentarnega gradiva. Zagotavlja se primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ oziroma brezkontaktna kartica), ki beleži dostope posameznikov do območja. Območje je varovano z video nadzornim sistemom. Vrata v prostore so lahko opremljena s slepo kljuko (možen dostop samo z izbranim sredstvom kontrole dostopa) in mehanizmom za samozapiranje. Prostori, kjer se hranijo osebni podatki in poslovna skrivnost, so lahko izven delovnega časa nadzorovani z načini tehničnega varovanja (kontrola vstopnih točk s protivlomnim alarmom, varnostno službo, videonadzornim sistemom za zagotavljanje kontrole vhoda).

- Območje komunikacijskega sistema (komunikacijske omare, komunikacijski vodi itd.)

Območje komunikacijskega sistema je namenjeno prenosu informacij. Zagotavlja se primerno varovanje, da je območje zaščiteno pred prestrezanjem komunikacij. Območje komunikacijskega prostora je lahko razdeljeno in obsega lastne prostore ali omare, ki ne smejo biti postavljene v območje javnega dostopa oziroma dostopne nepooblaščenim osebam.

Komunikacijski kabli, po katerih se prenašajo podatki, morajo biti zaščiteni pred prestrezanjem ali poškodbami. Nameščajo se v ustrezne kanale. Ožičenje ne sme predstavljati ovir pri gibanju. Vsi mrežni priključki, ki niso v uporabi, morajo biti neaktivni.

- Arhiv

Območje arhiva je namenjeno hrambi osebnih podatkov in poslovne skrivnosti ter dokumentarnega gradiva. Zagotavlja se primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ, brezkontaktna kartica itd.) za pooblaščene osebe.

2.3 Politika čiste mize

Zaposleni ne smejo puščati nosilcev podatkov (fizični izvodi, elektronski izvodi) z osebnimi podatki ali poslovno skrivnostjo na pisarniških mizah ali drugih mestih, kjer so dostopni nepooblaščenim osebam. Nosilce podatkov morajo uporabniki varno shraniti po končanem delovnem času oziroma ko dlje časa niso fizično prisotni v prostoru. Izven delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov z osebnimi podatki ali poslovno skrivnostjo, zaklenjena ali drugače varovana, računalniška oprema pa fizično in programsko varovana.

2.4 Politika praznega zaslona

Nepooblaščenim osebam mora biti onemogočen vpogled na računalniške zaslone. Vpogled lahko v posameznih primerih dovolijo zaposleni, če gre za obdelavo podatkov o uporabniku storitev, ki mora imeti vpogled v svoje osebne podatke.

Ob odhodu s svojega delovnega mesta morajo zaposleni vključiti ohranjevalnik zaslona in zakleniti računalnik. Čas neaktivnosti uporabnika, po katerem se mora avtomatično vključiti ohranjevalnik zaslona je največ 15 minut, računalnik pa samodejno zakleniti. Ob koncu delovnega časa se mora zaposleni odjaviti iz informacijskega sistema.

2.5 Odstranjevanje podatkov

Vsi nosilci podatkov z osebnimi podatki in poslovno skrivnostjo, se morajo uničiti na način, ki onemogoči branje vseh ali dela uničenih podatkov. Zaposleni nosilcev podatkov ne smejo odmetavati v koše za smeti. Za odstranitev podatkov se mora pripraviti primerne mehanizme (uničevanje, komisijski zapisnik o uničenju ipd.), ki zagotavljajo, da ne more priti do zlorabe podatkov.

2.6 Politika proti zlorabi opreme računalniškega informacijskega sistema

Vzdržuje se popis sredstev informacijskega sistema. Vsaka predaja ali sprejem opreme morata biti zabeležena. Vsa oprema ima identifikacijske oznake. Popis sredstev se preverja najmanj 1-krat letno. Za premeščanje računalniške opreme je zadolžena pooblaščena oseba, ki vodi evidenco o opremi informacijskega sistema in beleži spremembe v informacijskem sistemu.

3 POLITIKA NADZORA DOSTOPA DO APLIKACIJ, INFORMACIJ IN SISTEMOV

3.1 Namen

Politika nadzora dostopa določa pravila in postopke dodeljevanja pravic in pooblastil za dostop do informacij, aplikacij in sistemov ter odgovornosti pri njihovem izvajanju. Pravila in postopki omogočajo nadzor nad dostopi do informacijskega sistema ter zmanjšajo možnost nepooblaščenega dostopa, ki ima lahko za posledico razkritje, izgubo ali okvaro podatkov.

Pravila dostopov morajo biti usklajena z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje dejavnosti. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki se tičejo zaščite dostopov do informacij in storitev. Politiko nadzora dostopa je potrebno pregledovati in prilagajati ob spremembah procesov, občutljivosti informacij in informacijskega sistema.

3.2 Dostop do aplikacij in informacij

Dostop do aplikacij in informacij je omejen s sistemom overjanja. Način overitve je odvisen od varnostnih zahtev aplikacije, izvajati pa se mora najmanj z uporabo uporabniškega imena in gesla oziroma večfaktorske avtentikacije. Za dostop do ključnih, krmilnih ali nadzornih sistemov je potrebno uporabljati večfaktorsko avtentikacijo, če je to tehnično mogoče, ali pa je potrebno ustrezno izolirati sistem, da je možnost nepooblaščenega dostopa čim manjša.

Uporabljajo se posamične dostopne pravice (digitalna potrdila, enkratna gesla ali stalna gesla). Uporabnik se pred delom prijavi v aplikacijo, po uporabi pa iz nje odjavi. Sistem omogoča bodisi samodejno zaklepanje po 15 minutah neaktivnosti uporabnika bodisi ročno zaklepanje delovne postaje s strani uporabnika.

Pravice za dostop se uporabniku določi glede na njegovo vlogo in delovno mesto. Odobrene in dodeljene pravice uporabniku omogočajo, da dostopa do aplikacij in podatkov, ki jih potrebuje za izvajanje svojega dela.

3.3 Dostop do sistemov

Na sistemu obstaja en administratorski račun, katerega geslo je shranjeno in namenjeno uporabi v nujnih primerih, kot to opredeljuje Politika upravljanja in varovanja gesel. Oddaljeni dostop do sistemov je za vse pogodbene sodelavce nadzorovan s t.i. PAM (Privileged Access Management) orodjem preko VPN dostopa. Zaposleni uporabljajo večfaktorsko avtentikacijo za oddaljeni dostop.

Ostali administratorji imajo vsak svoj uporabniški račun, ki ima administratorske pravice, in uporabniški račun z običajnimi uporabniškimi pravicami (v Windows okolju člani skupine administrators, v Linux okolju Group ID = 0).

Oddaljeno povezovanje sistemskih administratorjev na računalniške naprave zaposlenih mora biti nadzorovano. Ob vzpostavitvi oddaljene povezave sistemskega administratorja na profil zaposlenega, je zaposlenemu na voljo potrditev ali zavrnitev vzpostavitve oddaljenega dostopa.

3.4 Dodelitev pravic dostopa

Pooblaščena oseba za kadre sproži ob prihodu novo zaposlenega postopek za dodelitev pravic dostopa. Pravice dostopa do informacij, aplikacij in sistemov, ki jih novo zaposleni potrebuje

glede na dodeljeno delovno mesto, določi in odobri njegov nadrejeni. Odobreno zahtevo za dodelitev dostopa se posreduje skrbnikom informacijskega sistema, ki so zadolženi za dodeljevanje in ukinjanje pravic dostopa.

Zahteva za uporabniški dostop mora vsebovati naslednje podatke:

- komu se dostop omogoči – ime, priimek
- kdaj naj se mu dostop omogoči
- do katerih informacij, aplikacij in sistemov potrebuje dostop
- ali potrebuje VPN dostop
- za kakšno trajanje naj bo dostop omogočen (do prenehanja delovnega razmerja, za določeno dobo)

Skrbniki informacijskega sistema dodelijo zahtevane pravice dostopa, nato pa obvestijo pooblaščeno osebo za kadre, da so bile pravice urejene.

Ob prihodu novo zaposlenega skrbnik informacijskega sistema sporoči vsa uporabniška imena in gesla, ki jih novi uporabnik potrebuje. Preden skrbnik informacijskega sistema izroči geslo uporabniku, ga mora še dodatno seznaniti s pravicami in odgovornostmi uporabe gesla za dostop do sistemov (opredeljeno v Politiki upravljanja in varovanja gesel).

Skrbnik informacijskega sistema ne sme zlorabljati poznavanja gesel uporabnikov v namene lastne uporabe ali za posredovanje tretji osebi. Uporabniško ime je uporabnikom dodeljeno trajno oziroma do preklica.

Dostop do podatkov, aplikacij in sistemov je lahko časovno neomejen in je lahko v primeru zlorab predčasno odvzet.

Skrbnik informacijskega sistema je dolžan voditi seznam uporabnikov z odobrenimi dostopi ter datumi dodelitve in ukinitve pravic. Seznam se uporabi kot osnovo za ukinitev vseh pravic dostopa pri odhodu zaposlenega.

Pooblaščena oseba za kadre vodi spremembe dostopnih pravic uporabnika v njegovi personalni mapi.

3.5 Ukinitev pravic dostopa

Pravice dostopa se uporabniku ukinejo v primeru zlorabe pravic ali ob prekinitvi delovnega razmerja.

V primeru zlorabe pravic pošlje nadrejeni zahtevek za ukinitev ali omejitev pravic dostopa. Ob prekinitvi delovnega razmerja nadrejeni pošlje pooblaščeni osebi za kadre zahtevek za ukinitev vseh pravic, ki so bile zaposlenemu dodeljene ob zaposlitvi in tekom njegovega dela. V zahtevku za ukinitev ali omejitev pravic se posreduje tudi datum prenehanja dela oziroma datum, ko se zaposlenemu ukinejo ali omejijo pravice.

Seznam vseh pravic, ki so bile zaposlenemu dodeljene ob prihodu v družbo ali med zaposlitvijo, je razviden iz seznama uporabnikov z odobrenimi dostopi, ki ga vodi skrbnik informacijskega sistema. Skrbnik informacijskega sistema po prejetem zahtevku za ukinitev pravic dostopa ukine uporabniški račun za dostop do omrežja, geslo za VPN dostop, ukine vse ostale pravice dostopa do aplikacij, sistemov ali podatkov (razvidno iz seznama uporabnikov z odobrenimi dostopi).

Ko so vse pravice dostopa ukinjene, skrbnik informacijskega sistema o tem obvesti pooblaščeno osebo za kadre in uporabnikovega nadrejenega ter ukinitev pravic evidentira v seznam uporabnikov z odobrenimi dostopi.

Izjemoma se lahko delavcu odvzamejo pravice takoj, ko delavec odpove pogodbo o zaposlitvi, če njegov nadrejeni oceni, da je to potrebno. Nadrejeni mora o tem obvestiti pooblaščeno osebo za kadre, ki nato sproži zgoraj opisan postopek za ukinitev pravic dostopa.

Skrbnik informacijskega sistema, ki skrbi za dodeljevanje in odvzem pravic periodično (vsaj na 6 mesecev), preverja, ali so bili za vse zaposlene, ki so v tem mesecu prenehali delovno razmerje, prejeti vsi zahtevki za odvzem pravic. V primeru neskladja o tem obvesti pooblaščeno osebo za kadre. Za vse ključne, krmilne in nadzorne sisteme morajo obstajati revizijske sledi uporabniških računov, ki so do njih dostopali, za najmanj 6 mesecev.

4 POLITIKA UPRAVLJANJA IN VAROVANJA GESEL

4.1 Namen

Namen dokumenta je predpisati obveznosti in pravila za varno ravnanje z gesli, redno menjavo in izbiro kvalitetnih gesel z namenom zmanjševanja tveganja zlorabe gesel, nepooblaščenega dostopa, ogrožanja ali kraje informacij.

4.2 Varovanje gesel

Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov odgovorni za vse akcije, ki se zgodijo z uporabo njihove identitete.

Uporabniki s svojimi osebnimi gesli ravnajo kot s strogo zaupnimi informacijami in jih ne smejo razkrivati oziroma posojati drugim osebam. Če zaposleni zasledi malomarno ali zlonamerno ravnanje z gesli, to takoj sporoči pooblaščeni osebi. Geslo mora uporabnik spremeniti takoj, če obstaja sum na razkritje gesla, in o tem obvesti pooblaščeno osebo.

Uporabniki pri izbiri gesel upoštevajo osnovna varnostna pravila. Geslo ne sme vsebovati besed iz slovarja, imen in priimkov uporabnika in družinskih članov, katerekoli oblike datuma, imena, oznake ali številke družbe, zaporednih števil.

Začasna gesla je zaposlenim potrebno pošiljati oziroma izročati na varen način.

Skrbnik informacijskega sistema, ki je odgovoren za dodelitev začasnega gesla, uporabniku ustno sporoči geslo, ki ga uporabnik spremeni ob prvi prijavi. Gesla zaposleni ne smejo zapisovati na papir ali shranjevati na kakršenkoli drug način, ki bi drugi osebi lahko omogočil dostop do gesla.

Če uporabnik geslo pozabi, mu skrbnik informacijskega sistema dodeli novo začasno geslo, ki ga uporabnik spremeni ob prvi prijavi.

4.3 Izbira in menjava uporabniških gesel

Pri izbiri in menjavi gesel so uporabniki dolžni upoštevati naslednja pravila:

- izbira se gesla z najmanj 12 znaki,
- geslo je sestavljeno iz najmanj 3 različnih znakov, od katerih je vsaj ena številka,
- gesla ne vsebujejo šumnikov.

V kolikor se uporablja večfaktorska avtentikacija, so lahko gesla manj kompleksna, to določata skrbnik informacijskega sistema in pooblaščena oseba.

4.4 Upravljanje in varovanje administratorskih gesel

Pri izbiri in menjavi gesel je zaželeno, da skrbniki informacijskih sistemov upoštevajo naslednja pravila:

- administratorska gesla naj imajo vsaj 14 znakov,
- gesla naj vsebujejo velike in male črke, števila in simbole.

V kolikor se uporablja večfaktorska avtentikacija, so lahko gesla manj kompleksna, to določata skrbnik informacijskega sistema in pooblaščena oseba.

Vsa administratorska gesla sistemov in aplikacij je potrebno shraniti, da se v nujnih primerih zagotovi možnost dostopa do sistemov tudi v odsotnosti skrbnika informacijskega sistema. Vsa administratorska gesla se hranijo v zaprtih kuvertah, ki so shranjene tako, da je

onemogočen dostop nepooblaščenim osebam. Na kuverto je potrebno napisati ime sistema oziroma aplikacije in datum, ko je bilo geslo zadnjič spremenjeno. Zaprto kuverto podpiše uporabnik gesla, ki je geslo shranil. V kuverti je zapisano, za katero administratorsko geslo gre ter uporabniško ime in geslo. Ob dodelitvi ali menjavi gesla skrbnik informacijskega sistema kuverto izroči pooblaščeni osebi, ki jo shrani tako, da je ustrezno zavarovana pred nepooblaščenimi dostopi. Odprtje katerekoli kuverte z geslom v primeru nujnega posega se mora zabeležiti v evidenčni list. Zapisati je potrebno datum in čas odprtja kuverte z geslom, kdo je odprl kuverto in kdo je dostopal do gesla. Geslo mora skrbnik informacijskega sistema v najkrajšem možnem času spremeniti.

Redna menjava gesla je zahtevana s strani informacijskega sistema, če sistem to omogoča.

5 POLITIKA VAROVANJA V ZVEZI Z OSEBJEM

5.1 Namen

Dokument predstavlja okvir za upravljanje izvajanja varnostnih postopkov ter dolžnosti in pravic za zaposlene in uporabnike informacijskega sistema.

- Varnostne politike

Vsi zaposleni in uporabniki informacijskega sistema so dolžni upoštevati vse dokumente sistema za upravljanje varovanja informacij (v nadaljevanju: SUVI).

Za izvajanje primernih varnostnih ukrepov so zadolženi zaposleni in ostali uporabniki, ki dostopajo do informacij in informacijskega sistema, vodstvo družbe pa je odgovorno za izvajanje mehanizmov varovanja informacij v celoti in za zagotovitev potrebnih virov, ki omogočajo primerno vodenje SUVI.

Vodstvo družbe je dolžno poskrbeti, da so dokumenti SUVI ustrezno objavljeni, tako da so varnostne politike na vpogled vsem zaposlenim in uporabnikom informacij in informacijskega sistema.

Vsako neupoštevanje pravil politik varovanja informacij in pripadajočih dokumentov SUVI šteje za kršitev pogodbe o delu ali pogodbe o sodelovanju in se kot tako tudi sankcionira.

5.2 Izobraževanje, usposabljanje in preverjanje

Vsi zaposleni in uporabniki informacijskega sistema morajo biti ustrezno izobraženi glede določil dokumentacije SUVI. Za izobraževanje je zadolžena pooblaščena oseba za kadre.

Izobraževanje se mora opravljati ob prihodu novega zaposlenega ali uporabnika informacijskega sistema ter vsaj 1-krat letno (osebno), obdobna ozaveščanja (preko e-pošte), phishing testi (vsaka dva meseca) oziroma takrat, ko je to potrebno zaradi spremembe varnostne politike, postopkov ali navodil. Izobraževanja se morajo udeležiti vsi zaposleni.

Preverjanje izobraževanj oziroma usposabljanj se lahko izvaja z načini preverjanja znanja udeležencev izobraževanj oziroma usposabljanj. Pooblaščena oseba lahko zahteva primerno poznavanje dokumentacije SUVI za zagotovitev primernega načina dela zaposlenih.

5.3 Varovanje informacij za zaposlene

Varovanje informacij se začne že pred samo zaposlitvijo ali uporabo informacijskega sistema, traja ves čas zaposlitve ali uporabe informacijskega sistema in se mora zagotavljati tudi po koncu zaposlitve ali uporabe informacijskega sistema.

- Pred zaposlitvijo ali uporabo informacijskega sistema

Pred zaposlitvijo ali uporabo informacijskega sistema in informacij mora pooblaščena oseba za kadre zagotoviti vpogled v dokumentacijo SUVI ter bodočemu novo zaposlenemu ali uporabniku informacijskega sistema in informacij dati v podpis Izjavo o zaupnosti ali pa mora to biti del pogodbe o zaposlitvi.

V pogodbi o zaposlitvi ali uporabi informacijskega sistema in informacij morajo biti jasno opredeljena načela varovanja informacij oziroma mora biti podan sklic na dokumentacijo SUVI in sankcije v primeru izgube, uničenja ali zlorabe informacij.

- Med zaposlitvijo ali uporabo informacijskega sistema

Pooblaščena oseba lahko preverja, ali zaposleni upoštevajo vsa določila dokumentacije SUVI in v primeru neupoštevanja sprejema ustrezne ukrepe. Vse spremembe, ki vplivajo na delo ali varovanje informacij, morajo biti posredovane vsem zaposlenim in uporabnikom informacijskega sistema.

Pripravljeni morajo biti postopki v primeru kršenja določil dokumentacije SUVI.

- Po prekinitvi zaposlitve ali uporabe informacijskega sistema

Odgovornosti in obveznosti, ki veljajo tudi po koncu zaposlitve, morajo biti vključene v pogodbe z zaposlenimi ali uporabniki informacijskega sistema in informacij.

Vsi zaposleni ter uporabniki informacijskega sistema in informacij morajo ob koncu zaposlitve ali pogodbe vrniti vsa sredstva informacijskega sistema, ki so jih prejeli v uporabo. Vsem zaposlenim ter uporabnikom informacijskega sistema je ob koncu zaposlitve potrebno odvzeti pravice fizičnega in logičnega dostopa do informacij in zmogljivosti za obdelavo informacij.

- Odgovornost

Vodstvo družbe je odgovorno za vse kršitve varnostnih politik s strani zaposlenih ali uporabnikov informacijskega sistema, v kolikor nima vpeljanega, izvajanega in vzdrževanega SUVI.

Vsako neupoštevanje varnostnih politik s strani zaposlenih ali uporabnikov informacijskega sistema mora biti ustrezno obravnavano v skladu s Politiko upravljanja varnostnih incidentov. Vodstvo družbe mora zagotavljati vsem zaposlenim primerna izobraževanja in dostop do dokumentacije SUVI. Vsako odstopanje od navedenega predstavlja neskladnost vodenja SUVI.

6 POLITIKA REVIZIJSKIH SLEDI

6.1 Namen

Politika revizijskih sledi določa pravila in postopke zagotavljanja sledljivosti dostopov do podatkov in informacijskih sistemov. Pravila in postopki omogočajo preverjanje dostopa do podatkov in sistemov v primeru zlorabe oziroma nepooblaščenega dostopa, ki ima lahko za posledico razkritje podatkov, med katere sodijo osebni podatki in poslovna skrivnost. Določitev pravil temelji na klasifikaciji informacij, veljavni zakonodaji in pogodbenih obveznostih, ki zadevajo zaščite dostopov do informacij in storitev. Politiko revizijskih sledi je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

6.2 Politika revizijskih sledi

Na sistemih morajo biti vzpostavljene revizijske sledi, ki omogočajo zagotavljanje sledljivosti naslednjih dogodkov:

- obdelav podatkov v skladu z Zakonom o informacijski varnosti,
- obdelav podatkov v skladu z Zakonom o varstvu osebnih podatkov,
- aktivnosti uporabnikov z administrativnimi pravicami,
- uspešne in neuspešne prijave v sisteme,
- dostope do revizijskih sledi.

Za vsak dogodek je potrebno opredeliti podatke, ki se beležijo, da je možno naknadno zagotoviti ustrezno sledljivost dogodkov, oziroma ugotoviti kdo, kdaj in kaj je storil.

Revizijske sledi je potrebno zaščititi pred nepooblaščenih dostopom in spreminjanjem.

Za namene revizijskih sledi nad gradivom v digitalni obliki, ki je zajeto v ISUD (Informacijski sistem za upravljanje z dokumenti), se hrani revizijska sled dostopa do gradiva (vpogled v dokument). Za ključne, krmilne in nadzorne sisteme se mora revizijska sled hraniti najmanj 6 mesecev.

Pogostost pregledovanja revizijskih sledi se za posamezen računalniški sistem in aplikacijo določi na osnovi analize tveganja. Za ključne, krmilne in nadzorne sisteme se mora pregled izvajati najmanj na 6 mesecev.

6.3 Sledljivost obdelav podatkov

Sledljivost obdelav podatkov mora biti primerna obdelovanim podatkom in se uporablja za vse podatke v ključnih, krmilnih in nadzornih sistemov (Zakonom o informacijski varnosti), osebne podatke (Zakon o varstvu osebnih podatkov) in poslovne skrivnosti.
Za informacije, ki so označene javno, sledljivost sprememb ni potrebna.

- Sledljivost posredovanja podatkov izven informacijskega sistema

Upravljavec osebnih podatkov mora za vsako posredovanje osebnih podatkov (izven informacijskega sistema) zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja poslovne skrivnosti ali osebnih podatkov. Prejemnik osebnih podatkov pa mora znotraj svoje družbe nato zagotoviti notranjo sledljivost prejetih osebnih podatkov.

- ### Hramba podatkov o vpogledih v podatke

Podatki o dostopih (vpogledih) morajo obstajati, morajo biti avtentični in dosegljivi za namene inšpekcijskih postopkov. Podatki se hranijo do zaključka hrambe oziroma do uničenja dokumentacije.

- ### Čas hrambe podatkov o vpogledih v osebne podatke

Zbirko vpogledov v osebne podatke se lahko uniči šele po šestih letih (razen če zakon ne določa drugačnega roka hranjenja) pod pogojem, da vanjo v tem obdobju ni nihče vpogledal.

7 POLITIKA ZAGOTAVLJANJA KAKOVOSTI INFRASTRUKTURE

7.1 Namen

Politika zagotavljanja kakovosti infrastrukture določa potrebno infrastrukturo za informacijski sistem. Potrebna infrastruktura zagotavlja primerno razpoložljivost informacijskega sistema za vse uporabnike. Določitev kakovosti infrastrukture temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki se tičejo zaščite dostopov do informacij in storitev. Politiko zagotavljanja kakovosti infrastrukture je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

7.2 Infrastruktura

Informacijski sistem se varuje s primernimi ukrepi in zagotavlja njegovo delovanje s pomočjo potrebne infrastrukture. Posamezni deli informacijskega sistema morajo biti podprti s primerno infrastrukturo, odvisno od razpoložljivosti, ki jo morajo zagotavljati.

- Informacijski sistem v območju upravnih pisarn (pisarne oziroma prostori družbe, kjer se nahajajo podatki ali sredstva informacijskega sistema (delovne postaje, prenosniki ipd.))

Za uporabniško računalniško opremo, ki je v območju upravnih pisarn, se zagotavlja nizko stopnjo razpoložljivosti (ni potrebne redundance). Računalniške naprave naj bodo nameščene na pisalnih mizah oziroma v območju, kjer je možnost fizičnega poškodovanja manjša (dvignjene od tal ipd.). Komunikacijski in električni kabli morajo biti speljani po kabelskih kanalih do računalniških naprav.

- Informacijski sistem v območju računalniškega IS

Računalniška oprema, ki je v območju računalniškega IS, mora zagotavljati visoko stopnjo razpoložljivosti. Zagotavlja se brezprekinitveno napajanje, ki omogoča neodvisno napajanje v primeru prekinitev električnega toka ter agregat, ki zagotavlja nadomestno napajanje. V območju morajo biti okoljski parametri (temperatura, vlažnost) v skladu s specifikacijami proizvajalca opreme, sicer je obvezna uporaba klimatske naprave. Priporoča se podvojen sistem klimatskih naprav. Računalniške naprave morajo biti zaščitene pred udari električnega toka (prenapetostna zaščita). Računalniške naprave morajo biti nameščene tako, da je možnost fizičnega poškodovanja manjša (zaščita pred izlivom vode, požarom, nenamernim poškodovanjem). Na računalniško opremo ni dovoljeno polagati drugih naprav in predmetov. Računalniška oprema je zavarovana s primernim sistemom za gašenje in obveščanjem o kritičnih dogodkih (senzorji za dim, previsoko temperaturo ter vdor vode). Komunikacijski in električni kabli morajo biti speljani do računalniških naprav na način, da ne moti dostopa in da je možnost poškodovanja čim manjša.

Zagotavlja se redno čiščenje območja, da se zmanjša možnost zamašitve hladilnih rež.

Agregat, UPS in klimatske naprave se pregledujejo skladno z navodili proizvajalca. Agregat je preverjan tedensko, UPS mesečno, klimatske naprave pa najmanj letno.

- Območje komunikacijskega sistema (komunikacijske omare, komunikacijski vodi itd.)

Komunikacijska oprema, ki je v območju komunikacijskega sistema, mora zagotavljati visoko stopnjo razpoložljivosti. Za uporabo komunikacijske opreme se mora zagotoviti brezprekinitveno napajanje v primeru prekinitev električnega toka. Komunikacijske naprave morajo biti zaščitene pred udari električnega toka (prenapetostna zaščita). Komunikacijske naprave morajo biti nameščene tako, da je možnost fizičnega poškodovanja manjša (zaščita

pred izlivom vode, požarom, nenamernim poškodovanjem). Na komunikacijsko opremo ni dovoljeno polagati drugih naprav in predmetov. Komunikacijski kabli, po katerih se prenašajo podatki, morajo biti zaščiteni pred prestrezanjem ali poškodbami in nameščeni v ustrezne kanale.

7.3 Zagotavljanje kakovosti infrastrukture

Vsa podporna infrastruktura (električna energija, hlajenje, komunikacijske povezave) mora biti pregledana s strani pooblaščenih oseb v primernem časovnem intervalu. Vsaka odpoved mora biti zabeležena in na podlagi tega sprejet primeren ukrep, ki zagotavlja izboljšavo. Vse odpovedi morajo biti zabeležene v zapisniku notranje presoje. Pregled kakovosti infrastrukture se izvaja najmanj 1-krat letno.

8 POLITIKA VARNOSTNEGA KOPIRANJA

8.1 Namen

Namen varnostnega kopiranja podatkov je zagotoviti rezervno kopijo podatkov in omogočiti ponovno vzpostavitev sistema in uspešno nadaljevanje dela po množici različnih dogodkov oz. varnostnih incidentov, ki povzročijo poškodovanje ali izgubo podatkov – kot so problemi s strojno opremo, problemi s programsko opremo, človeške napake, naravne nesreče ipd. Zato se vsi pomembni elektronski podatki redno shranjujejo na medije daljše trajnosti.

8.2 Navodilo za izvajanje in ravnanje

Izdelava varnostnih kopij in zmožnost ponovne vzpostavitve sistema in restavriranja podatkov je bistvenega pomena za neprekinjeno izvajanje dejavnosti. Varnostno kopiranje se izvaja skladno z analizo vpliva na poslovanje.

Izbira naprav in medijev za izdelavo varnostnih kopij ustreza količini podatkov, ki jih shranjujemo, in zahtevani hitrosti shranjevanja in restavriranja. Uporablja se tako način rednundance za ključne, krmilne in nadzorne sisteme, kot tudi shranjevanje na prenosnih medijih (trak). Mediji za shranjevanje podatkov oziroma ponovno instalacijo so ustrezno označeni, da jih je možno v čim krajšem času in pravilno uporabiti pri restavriranju podatkov. Mediji so varno shranjeni tako, da niso dostopni nepooblaščenim osebam, ter da niso izpostavljeni enakim grožnjam kot originalni podatki. Pri preizkušanju postopkov za restavriranje se preverja, ali je podatke možno restavrirati in sistem uspešno usposobiti za nadaljevanje z delom v času, ki ga določajo zahteve procesov.

8.3 Shranjevanje prenosnih medijev z varnostnimi kopijami

Prenosni mediji z varnostnimi kopijami so varno shranjeni, da niso dostopni nepooblaščenim osebam, ki bi z njihovo pomočjo lahko dobile dostop do podatkov. Prenosni mediji z varnostnimi kopijami podatkov se hranijo v drugem prostoru kot originalni podatki na način, da so zaščiteni pred ognjem in vdorom vode. Dostop do varnostnih kopij podatkov imajo pooblaščene osebe za varnostno kopiranje, ki jih določi oseba, odgovorna za delovanje informacijskega sistema družbe. Vsako shranjevanje varnostnih kopij se evidentira, pri čemer se zabeleži:

- kaj vsebuje varnostna kopija,
- čas izdelave varnostne kopije,
- enolična označba kopije,
- zapis o uspešnosti in neuspešnosti izdelave kopije.

Za shranjevanje in označevanje prenosnih medijev z varnostnimi kopijami podatkov so zadolžene odgovorne osebe za varnostno kopiranje podatkov. Na prenosnem mediju je označeno najmanj:

- ime sistema in specifična vrsta shranjenih podatkov,
- datum, ko so bili podatki prvič zapisani na medij (če se podatki na medij prepisujejo, se zapiše datum zadnje varnostne kopije),
- vrsta varnostne kopije.

Varnostne kopije podatkov se vsaj enkrat mesečno prenašajo na oddaljeno lokacijo, ki je v drugem območju naravnih nesreč (vsaj 30 km oddaljenosti). Predaja nosilcev z varnostnimi kopijami podatkov se izvrši na način, ki vključuje sprotno vodenje evidence varnostnih kopij na vseh lokacijah družbe.

Postopki varnostnega kopiranja so opredeljeni za vsak posamezen informacijski sistem v operativnih navodilih družbe.

8.4 Preverjanje varnostnih kopij

Odgovorne osebe za varnostno kopiranje podatkov enkrat na 6 mesecev preverijo, da se podatki dejansko nahajajo na označenih prenosnih medijih in da mediji niso poškodovani ali uničeni ter testirajo, ali bi bilo v primeru incidenta podatke mogoče restavrirati iz varnostnih kopij na prenosnih medijih. V ta namen se izvede popolno restavriranje naključno izbranega dela varnostne kopije podatkov. O potrditvi uspešnega restavriranja varnostnih kopij se napravi zapisnik.

8.5 Načrt za obnovo podatkov

Postopek uporabe varnostnih kopij pri morebitni potrebi po restavriranju informacijskih sistemov je naveden v naslednjih dokumentih:

Načrt obnove podatkov s strani vzdrževalca PIS. Pooblaščene osebe za dostop do varnostnih kopij.

8.6 Nadzor izvajanja

Izvajanje določil, navedenih v tem navodilu se preverja najmanj enkrat na 6 mesecev na notranjih presojah ali revizijah.

9 POLITIKA IZDELAVE IN HRAMBE DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA

9.1 Namen

Politika hrambe dokumentarnega in arhivskega gradiva določa pravila in postopke arhiviranja podatkov. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki se tičejo hrambe dokumentacije v družbi. Politiko izdelave in hrambe dokumentarnega in arhivskega gradiva je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

9.2 Čas hranjenja dokumentacije

Posamezne evidence se hranijo skladno s predpisi zakonodaje (področna energetska zakonodaja, Zakon o varstvu osebnih podatkov, davčna zakonodaja).

9.3 Izdelava in hramba dokumentacije

Družba hrani dokumentacijo v obliki fizičnih ali elektronskih izvodov. Vsa dokumentacija mora biti hranjena na način, kot je predpisano v Politiki fizične zaščite in fizičnega dostopa. Zagotavljati je potrebno primerno hrambo dokumentacije, da ne pride do poškodb ali uničenja dokumentacije oziroma zlorabe podatkov.

9.4 Izdelava in hramba dokumentacije v elektronski obliki

Za hrambo dokumentacije v elektronski obliki je potrebno zagotoviti primerne postopke elektronske hrambe (notranja pravila, zajem, pretvorba, pogoji pretvorbe in elektronske hrambe, usklajenost s tehnološkimi standardi) ter infrastrukturo (strojna in programska oprema, ponudniki opreme in storitev, registracija, certifikacija, nadzor). Infrastrukturo zagotavlja družba. V primeru izvajanja aktivnosti skupaj s pogodbenim sodelavcem, mora biti opredelitev varstva infrastrukture zagotovljena v pogodbi z izvajalcem storitve (npr. zunanji ponudnik ISUD (informacijski sistem za upravljanje dokumentarnega gradiva).

Vsa hramba dokumentarnega in arhivskega gradiva – dokumentacije v elektronski obliki – mora biti skladna z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih. Oblika zapisa mora zagotavljati ohranitev vsebine gradiva ter omogočati po obdobju 5 let pretvorbo v novo elektronsko obliko zapisa, ki bo takrat izpolnjevala pogoje varne hrambe gradiva. Nosilec podatkov mora zagotavljati vse pogoje varne hrambe gradiva in omogočati večje število prepisov s sedanjih na bodoče nosilce podatkov. Opredelitev mora biti zagotovljena v pogodbi z izvajalcem storitve (zunanji ponudnik ISUD).

Hramba nosilcev podatkov mora biti skladna z varnostnimi politikami in upoštevati določila zakonodaje glede okolja za hrambo in delovanja elektronskih nosilcev podatkov. Dostopnost podatkov in nosilcev podatkov mora biti omejena na pooblaščene osebe. Opredelitev mora biti zagotovljena v pogodbi z izvajalcem storitve (zunanji ponudnik ISUD).

Glede na vrsto dokumentarnega gradiva je potrebno zagotoviti primerno število varnostnih kopij na različnih lokacijah. Izvajati se mora stalna kontrola nosilcev zapisa. Opredelitev mora biti zagotovljena v pogodbi z izvajalcem storitve (zunanji ponudnik ISUD).

9.5 Uničenje dokumentacije

Pri uničenju izvirnega dokumentarnega gradiva mora biti prisotna tričlanska komisija. Uničenje gradiva mora biti evidentirano (zapisnik, popis gradiva za uničenje).

10 POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA PROGRAMSKE OPREME

10.1 Namen

Namen dokumenta je opredeliti postopek razvoja in vzdrževanja programske opreme, odgovornosti in naloge sodelujočih, način nadzora ter dokumentacijo, ki jo je potrebno pri tem izdelati.

Namen navodila je zagotoviti, da ima programska oprema zahtevano funkcionalnost, zanesljivost in učinkovitost, da izpolnjuje varnostne zahteve ter da testiranje in vpeljava programske opreme v produkcijsko okolje poteka nadzorovano in ne ovira procesov v produkcijskem okolju oziroma ne vpliva na produkcijske podatke.

10.2 Navodilo za izvajanje razvoja programske opreme

Razvoj programske opreme je projektno organiziran in se izvaja po predpisanih fazah, ki so opredeljene v nadaljevanju. V kolikor se za razvoj uporablja pogodbenega izvajalca, se upošteva tudi poglavja IZBIRA IZVAJALCA, IZDELAVA VZPOSTAVITVENEGA DOKUMENTA PROJEKTA, pri lastnem razvoju pa se teh dveh poglavij ne upošteva:

IZBIRA IZVAJALCA (v primeru uporabe pogodbenih sodelavcev)
Okvir za naročanje storitev pri pogodbenih sodelavcih postavlja veljavna zakonodaja.

V razpisni dokumentaciji se pri pogojih, ki jih mora izpolnjevati pogodbeni sodelavec, navede tudi zahteve glede sposobnosti izvajalca, da ustrezno varuje informacije, ki jih izvajalec lahko izkaže npr. s certificiranim sistemom upravljanja varovanja informacij (SUVI) ali s kadri s certifikati na področju upravljanja in revidiranja sistemov varovanja informacij.

IZDELAVA VZPOSTAVITVENEGA DOKUMENTA PROJEKTA (v primeru uporabe pogodbenih sodelavcev)

Izdela se vzpostavitveni dokument projekta, ki vsebuje:
Predstavitev projekta

- namen
- cilji
- predpostavke, omejitve, tveganja

Vsebina projekta

- prednosti nove programske opreme
- tehnične lastnosti
- varnostne zahteve

Organizacija projekta

- organizacijska shema in opis zadolžitev sodelujočih
- nadzor projekta: določi se kontrolne točke – preglede terminskega načrta in validacijo razvoja
- informacijska podpora za vodenje projekta

Načrt razvoja:

- izdelki
- terminski načrt z opisom aktivnosti
- plan resursov

IZDELAVA SPECIFIKACIJ
Pripravi se tehnični načrt oziroma **funkcionalne zahteve**, v katerih se opredeli:

- potrebne funkcionalnosti
- enolične specifikacije elementov programske opreme
- **varnostne zahteve**, ki vključujejo, niso pa izključno omejene na:
    - zahteve ob prijavi (uporaba enoličnih identifikatorjev kot to določa Politika nadzora dostopa)
    - funkcionalnosti, ki zagotavljajo varnost podatkov v fazi vnosa, obdelave, prenosa in hranjenja (mehanizmi validacije vhodnih in izhodnih podatkov, šifriranje itd.)
    - zahteve glede revizijskih sledi (opredeljeno v Politiki revizijskih sledi)
- načrt testiranja (priprava običajnih in mejnih testnih primerov)

IZVEDBA RAZVOJA PROGRAMSKE OPREME
Razvoj poteka v razvojnem okolju na računalniški opremi izvajalca, ki je prilagojena zahtevam razvoja. V skladu s Politiko upravljanja kakovosti in varnosti storitev tretjih strank je vodja projekta odgovoren, da izvajalca že pred začetkom razvoja seznani z določili varnostne politike, ki jih je izvajalec dolžan upoštevati.

Vodja projekta spremlja potek razvoja skladno z načrtom projekta ter ob kontrolnih točkah poroča sodelujočim na projektu. V primeru neskladnosti z načrtom projekta se projektni svet odloča o spremembi načrta, prekinitvi ali nadaljevanju projekta.

IZDELAVA DOKUMENTACIJE
Izdela se dokumentacija nove programske opreme, ki vsebuje vsaj:

- navodilo za namestitev (testne in produkcijske verzije)
- enolično oznaka nove verzije in opis sprememb nove verzije
- opis tehničnih zahtev za strojno in programsko opremo strežnika, na katerem bo nameščena nova programska oprema
- navodilo za testiranje
- uporabniški priročnik

TESTIRANJE
Testiranje programske opreme je obvezna faza pred prevzemom.
Skrbnik podatkov je odgovoren za pripravo testnih podatkov, ki so anonimizirani oziroma spremenjeni tako, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa. V nabor podatkov se po potrebi vključi podatke, pri katerih je bilo testiranje v preteklosti neuspešno.

Pogodbeni sodelavec v testnem okolju družbe testira osnovno funkcionalnost programske opreme v skladu z načrtom testiranja oziroma testnimi primeri, ki so bili opredeljeni v specifikacijah. Rezultate testiranja mora pogodbeni sodelavec vpisati v zapisnik testiranja. Zapisnik testiranja pogodbeni sodelavec podpiše in ga posreduje vodji projekta.

Rezultate testiranja se zapiše v zapisnik testiranja. V primeru ugotovljenih neustreznosti oziroma odstopanj od specifikacij, navedenih v pogodbi, vodja projekta uredi, da pogodbeni sodelavec napake oziroma odstopanja odpravi.

Ko se z ustreznim postopkom testiranja ugotovi, da izdelana programska oprema zagotavlja v pogodbi opredeljeno funkcionalnost, zmogljivost in varnostne zahteve, odgovorne osebe, ki so izvedle testiranja, s podpisom potrdijo zapisnik rezultatov testiranja.

SKLADNOST S PREDPISI
V kolikor se izvaja razvoj na ključnih, krmilnih ali nadzornih sistemih, je potrebno upoštevati vse zahteve Zakona o informacijski varnosti in podzakonskih aktov, vključno z varnostnim preverjanjem pred prehodom v produkcijo.

V kolikor se izvaja razvoj, ki vpliva na zajem in hrambo dokumentarnega ali arhivskega gradiva v digitalni obliki, se mora zagotoviti, da izvajalec programsko opremo certificira pri Arhivu RS.

PREVZEM
Za prevzem programske opreme je odgovoren vodja projekta, ki prevzame programsko opremo z ustrezno dokumentacijo ter preveri njeno ustreznost.

Prevzem programske opreme in dokumentacije potrdita vodja projekta in projektni svet s podpisom primopredajnega zapisnika.

NAMESTITEV PROGRAMSKE OPREME
Vodja projekta posreduje zahtevo za namestitev programske opreme v produkcijsko okolje osebi, ki je odgovorna za informacijski sistem. Zahtevi mora priložiti navodila za namestitev, tehnično dokumentacijo, programsko opremo in zapisnik rezultatov testiranja programske opreme.

Namestitev programske opreme v produkcijsko okolje sme opraviti le pooblaščeni sistemski skrbnik programske opreme ali informacijskega sistema.

Ob namestitvi programske opreme se izvede test ranljivosti.

UVAJANJE UPORABNIKOV
Izvede se usposabljanje uporabnikov, s katerim se jih usposobi za uporabo nove programske opreme.

10.3 Vzdrževanje programske opreme

V kolikor uporabniki pri delu s programsko opremo naletijo na težave oziroma napake, jih sporočijo na enak način kot vse ostale težave in napake delovanja informacijskega sistema. Pri prijavi napake ali težave mora uporabnik navesti:

- ob kateri akciji je prišlo do napake,
- kako se napaka odraža,
- če je možno tudi sliko zaslona v trenutku, ko se je napaka ali težava pojavila.

Če se ugotovi, da je napaka povezana z delovanjem aplikacije, se v reševanje vključi vodjo projekta, ki je bil odgovoren za razvoj programske opreme. Vodja projekta ugotovi vzrok za težavo ali napako in po potrebi v reševanje vključi pogodbenega sodelavca, ki je razvil programsko opremo. Če je vzrok za težavo ali napako take narave, da zahteva spremembo programske opreme, vodja projekta sproži postopek za razvoj nove verzije, ki se jo testira in vpelje v produkcijo v skladu z navodilom za razvoj programske opreme.

Za spremljanje ustrezne varnosti programske opreme se vsaj enkrat letno izvajajo vdorni testi (mdr. varnostno testiranje omrežja, zunanje varnostno testiranje, notranje varnostno testiranje, varnostno testiranje aplikacij, pregled arhitekture informacijskega sistema, testiranje zaznave in odziva varnostnih sistemov in VOC (t.i. Red Team test) ter CTI (Cyber Threat Intelligence) pregledi).

11 POLITIKA NADZORA SPREMEMB INFORMACIJSKEGA SISTEMA (PROGRAMSKE IN SISTEMSKE OPREME TER STROJNE OPREME)

11.1 Namen

Politika nadzora sprememb informacijskega sistema določa pravila in postopke spreminjanja informacijskega sistema. Pravila in postopki omogočajo natančen potek sprememb informacijskega sistema in nadzor, ki zagotavlja samo odobrene spremembe. Neodobrene spremembe imajo lahko za posledico nedelovanje informacijskega sistema, kar lahko povzroči nezmožnost zagotavljanja storitev uporabnikom.

Pravila in postopki nadzora sprememb informacijskega sistema morajo biti usklajeni z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje dejavnosti. Politiko nadzora sprememb informacijskega sistema je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

11.2 Nabava programske in sistemske opreme ter strojne opreme

Za nabavo se mora izdelati predlog s specifikacijami. V specifikacijah morata biti natančno določena zahtevana funkcionalnost in zmogljivost opreme, vključene pa morajo biti tudi varnostne zahteve iz Politike razvoja, spreminjanja in vzdrževanja programske opreme.

11.3 Namestitev programske in sistemske opreme ter strojne opreme

Programsko opremo je potrebno pred namestitvijo v produkcijsko okolje ustrezno testirati v testnem okolju, pri tem pa je pomembno, da se predvidi vse okoliščine, ki se bodo pojavile v produkcijskem okolju. Pred spremembami in migracijami se izdela varnostna kopija sistema, stari sistem se ohrani, da je možna povrnitev v prvotno stanje.

Vsa programska oprema mora ustrezati zahtevam in pogojem licenčnih predpisov. Skrbniki informacijskih sistemov so odgovorni za spremljanje veljavnosti oziroma poteka licenc in so dolžni sprožiti postopek za nabavo novih licenc (izda se predlog s specifikacijami za nabavo). Na računalniški IS je dovoljeno nameščati le odobreno programsko opremo, ki jo določi pooblaščena oseba. Kakršnokoli nameščanje druge programske opreme brez dovoljenja pooblaščenih oseb in mimo postopkov odobritve nove programske opreme je prepovedano.

Vsa programska in sistemska oprema ter strojna oprema mora biti nameščena s strani pooblaščenih oseb in usklajena z varnostnimi politikami. Pred spremembami strojne opreme se izdela varnostna kopija sistema, stari sistem se ohrani, da je možna povrnitev v prvotno stanje.

Pred namestitvijo v produkcijsko okolje se izvede varnostno testiranje (najmanj, ko se izvaja namestitev novega ali spremenjenega ključnega, krmilnega ali nadzornega sistema), če je sprememba vplivala na funkcionalnosti informacijskega sistema, ki bi lahko pomenile vpliv na varnost.

Uporabnike se predhodno obvesti o spremembah informacijskega sistema, ki bi lahko povzročile spremembe pri njihovem rednem delu.

11.4 Nadzor nad verzijami programske opreme

Vsaka spremenjena verzija programske opreme, ki jo nameščamo, mora biti enolično označena, da je zagotovljena sledljivost nad verzijami. Oznako verzije programske opreme določi razvijalec programske opreme. Potrebno je voditi evidenco verzij (pri razvijalcu ali v družbi).

11.5 Nadzor sprememb informacijskega sistema

Spremembe računalniškega IS se preverja na notranjih presojah, kjer se ugotavlja, ali so bile spremembe primerno vpeljane in zadostujejo primernemu nivoju informacijske varnosti. Za preverjanje se lahko uporabi mehanizme notranjih varnostnih pregledov.

12 POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO

12.1 Namen

Namen dokumenta je opredeliti mehanizme za zaščito pred zlonamerno programsko opremo in zmanjšati možnost, da bi le-ta ogrozila neoporečnost in zaupnost informacij in programske opreme.

12.2 Zaščita pred zlonamerno programsko opremo

Da bi komunikacijske segmente omrežja in strežnike zaščitili pred zlonamerno kodo in njenim nenadzorovanim razširjanjem, se mora zadostiti sledečim zahtevam:

- Uporablja se programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo v t.i. XDR orodjih ki omogočajo neprekinjeno spremljanje ranljivosti informacijskih sistemov. Omenjena programska oprema je nameščena na vse odjemalce. Za namestitev in nadzor je zadolžena pooblaščena oseba, ki programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo namesti na način, da je uporabniki ne morejo izključiti oziroma odstraniti.
- Uporabljena programska oprema za zaščito pred zlonamerno programsko opremo se redno neprekinjeno posodablja, prav tako pa se redno izvaja pregledovanje trdih diskov in prenosnih medijev (periodično najmanj 1x mesečno).

Razmejuje se lokalna omrežja oziroma ločuje dele omrežij, v katera so priključeni odjemalci, od delov omrežij, v katere so priključeni strežniki ter poslovna omrežja in OT omrežja. Omejujejo se neposredni administrativni dostopi iz uporabniških v strežniške dele omrežja ter med poslovnimi omrežij in OT omrežji. Med posameznimi segmenti se nahaja požarna pregrada, ki omogoča pregled prometa med segmenti.

V OT okolju se dodatno uporablja ADS za nadzor nad prometom.

13 POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV TRETJIH STRANK

13.1 Namen

Dokument predstavlja okvir za upravljanje kakovosti storitev tretjih strank. Namen dokumenta je opredeliti postopke, s katerimi družba zagotovi, da tretje stranke izvajajo dogovorjeno raven storitev in zagotavljajo ustrezno varnost informacij.

13.2 Pogodbeno urejanje razmerij s tretjimi strankami

Pogodba o izvajanju storitev, ki jo izvaja tretja stranka, opredeljuje opis storitev in predvideni rok trajanja oziroma dobo opravljanja teh storitev. Pri opisu storitev so opredeljeni cilji in vnaprej določene ravni izvajanja storitev, vključno z opredelitvijo preverljivih kriterijev za doseganje teh ravni, načinom poročanja ter pravico nadzorovanja pogodbenih obveznosti, lahko tudi s strani tretjih strank.

Določila o seznanjenosti in sprejemanju varnostnih zahtev za tretje stranke, ki jih določajo varnostne politike, se vključi v pogodbo ali doda kot samostojno prilogo.
Določila tretje stranke obvezujejo:

- Upoštevanja vseh zahtev skladno z Zakonom o informacijski varnosti in Zakonom o varstvu osebnih podatkov,
- da se zagotovi varnost ključnih, krmilnih in nadzornih informacijskih sistemov,
- da osebnih podatkov in poslovne skrivnosti do katere pridejo ne bodo posredovali drugim osebam,
- da jih bodo varovali tako, da bo preprečeno nepooblaščeno razkritje,
- da jih ne bodo uporabljali na kakršenkoli način, izven načina, dogovorjenega s pogodbo.

Pri tem se skladno s pogodbo izvaja varovanje skozi celotno obdobje sodelovanja in pa določeno obdobje po zaključku sodelovanja s tretjo stranko.

V pogodbo s tretjo stranko se vključi določbe, ki se nanašajo na:

- način poročanja ter obveščanja o varnostnih incidentih,
- postopke za zaščito sredstev za izvajanje storitev,
- zahteve glede varovanja podatkov,
- nadzor dostopa, vključno z dovoljenimi metodami dostopa tretje stranke,
- vodenje in dostopnost seznama izvajalcev, pooblaščenih za izvajanje storitev,
- obveznosti glede namestitve in vzdrževanja strojne in programske opreme tretje stranke ter zahtevanih fizičnih in logičnih nadzornih mehanizmov dostopa do sistemov, storitev in informacij,
- zahteve, da tretja stranka omrežje varuje pred grožnjami iz zunanjih omrežij z opremo, ki zagotavlja največjo možno varnost pred zlonamerno programsko opremo in zunanjimi vdori do sistemov, storitev in podatkov,
- zahteve, da bo tretja stranka na pisno zahtevo posredovala vse podatke, ki so v zvezi z zagotovitvijo varnosti sistemov, storitev in informacij za izvajanje storitev,

- pravico do revizijskega pregleda (družba si pridržuje pravico do preverjanja ravni varnosti, ki ga zagotavlja tretja stranka, z varnostnimi pregledi informacijskega sistema tretje stranke),
- varnost dobavne verige oziroma možnost vključitve podizvajalcev,
- načine zagotavljanja, da se vse osebe, ki so povezane z pogodbenim izvajanjem storitev, vključno s podizvajalci, zavedajo svojih obveznosti glede zagotavljanja ustrezne varnosti.

V pogodbo se vključi tudi določbe, ki določajo ukrepe v primeru kršitev obveznosti iz pogodbe in odgovornost pogodbenih strank oziroma sankcije.

Kjer je potrebno, se pri naročanju storitev pri tretji stranki dogovori o neprekinjenosti storitev, ki se morajo ohraniti tudi v primeru nepredvidenih dogodkov, npr. pri večjih okvarah ali nesrečah.

Pred sklenitvijo pogodbe mora osebje tretje stranke, ki bo izvajalo dela po pogodbi, podpisati izjavo o seznanitvi in sprejemanju varnostnih zahtev, ki so opredeljene v tej varnostni politiki.

13.3 Upravljanje sprememb pogodbenih storitev tretjih strank

Spremembe v zvezi z zagotavljanjem pogodbenih storitev se upravlja tako, da skrbnik pogodbe najmanj enkrat letno preverja postopke tretje stranke. Skrbnik pogodbe je odgovoren za:

- informiranje tretje stranke o relevantnih določbah varnostne politike,
- nadzor in spremljanje ravni izvajanja storitev in varovanja informacij tretje stranke,
- pregledovanje poročil in zapisov tretje stranke,
- spremljanje sprememb pri izvajanju storitev in po potrebi sprožitev postopka za spremembo postopkov oziroma dokumentov varnostne politike in revizijo pogodbe s tretjo stranko.

13.4 Politika nadzora dostopa tretjih strank do informacijskega sistema in informacij

Ko se pojavi potreba po dostopu tretjih strank do informacij ali informacijskega sistema, se najprej izvede analizo tveganja in ugotovi potrebne varnostne ukrepe. Dostop tretjim strankam do informacij in informacijskega sistema ni dovoljen, dokler niso implementirani ustrezni varnostni in nadzorni mehanizmi in niso stopila v veljavo potrebna interna pravila in pogodba, ki definira pogoje dostopa.

Pravila za določanje dostopov opisujejo načine dostopa in omogočajo nadzor nad dostopi do informacij in informacijskega sistema. Osnova za izdelavo pravil je varnostna razvrstitev podatkov, ki jo določa Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami.

Tretjim strankam omogočimo dostop do samo tistih informacij in sistemov, ki jih nujno potrebujejo pri svojem delu. Na ta način preprečujemo nepooblaščen dostop.

Tretje stranke pred začetkom dela seznanimo z varnostnimi politikami, ki jih je tretja stranka dolžna upoštevati. Pogoji sodelovanja in ukrepi nadzora so zapisani v pogodbi med tretjo stranko in družbo. S podpisom pogodbe se tretja stranka obveže spoštovati in upoštevati varnostne predpise in varovati vse podatke, do katerih imajo dostop.

- Logični dostop do informacijskega sistema in informacij

Za odobritev in izvedbo postopka za dostop v omrežje za tretje stranke je potrebno pripraviti zahtevek ali izdelati drug dokument, ki vsebuje vse predpisane podatke. Zahtevek za pogodbenega sodelavca izpolni vodja organizacijske enote, v kateri je tak dostop potreben.

Za tretje stranke se pripravi poseben izoliran segment omrežja, kamor se lahko priključijo. Od tam imajo omejen (filtriran) dostop preko požarne pregrade do omrežja in sicer samo s servisi, ki so potrebni in odobreni za njihovo delo in samo do notranjih mrežnih virov, ki so specificirani v odobrenem zahtevku in potrebni za njihovo delo.

Tretje stranke se pri vstopu v omrežje overijo z enoličnim identifikatorjem. Vsi dostopi tretjih strank do informacijskega sistema se beležijo ves čas sodelovanja s tretjo stranko in pregledujejo enkrat mesečno.

- Vodja organizacijske enote, ki potrebuje dostop za tretje stranke, izpolni zahtevek. V zahtevku pa navede:
  - osebne podatke kontaktne osebe tretje stranke (ime, priimek, telefonska številka),
  - morebitne časovne omejitve dostopa,
  - način dostopa,
  - namen oddaljenega dostopa (do katerih mrežnih virov in mrežne opreme potrebuje dostop),
  - tehnične podatke (IP številka).
- Odgovorna oseba za informacijski sistem pregleda zahtevek in dopolni parametre obrazca.
- Priporočljivo je, da se za dostop tretjih strank glede na ocenjeno stopnjo tveganja pripravijo ločeni segmenti omrežja, ki so povezani z omrežjem preko požarne pregrade.
- Tretji stranki se omogoči dostop le do tistih servisov, ki so potrebni za delo tretje stranke – v skladu z odobrenim zahtevkom.
- Določi se gesla za dostop do notranjih mrežnih virov za tretjo stranko – v skladu z odobrenim zahtevkom.
- Skrbnik informacijskega sistema izvede test dostopa.
- Tretja stranka podpiše zahtevek za dostop in s tem potrdi prevzem gesel ter seznanjenost z varnostnimi pravili dostopa.
- Zahtevek se arhivira na ustrezno mesto.

Tretjim strankam se prekine dostop v omrežje takoj, ko dostopa do informacijskega sistema ne potrebujejo več oziroma najpozneje, ko preneha pogodbeno razmerje med družbo ter tretjo stranko.

Čas prekinitve dostopa za tretjo stranko sporoči skrbnikom informacijskega sistema vodja organizacijske enote, ki je odobril dostop. Če je že vnaprej znano, da bo dostop omogočen za določeno dobo, se predviden datum prekinitve dostopa napiše že na zahtevo.

Dostop v omrežje se prekine v primeru kršitve določil varnostnih predpisov in navodil. Če se pojavi sum kršitve varnostnih predpisov in navodil, se dostop v omrežje začasno onemogoči, dokler se ne ugotovi dejanskega stanja kršitve.

- Fizični dostop do informacijskega sistema in informacij

Vzdrževanje opreme lahko izvajajo le pooblaščene tretje stranke, s katerimi je sklenjena pogodba z ustreznimi členi glede varovanja informacij. Dostop tretje stranke do strojne opreme je vedno nadziran. Vzdrževalna dela se izvajajo na mestu, kjer se oprema nahaja. Če to ni mogoče, se odstrani nosilec podatkov iz opreme in se ga varno shrani. Če podatkov ni mogoče odstraniti ali kako drugače zaščititi, mora biti postopek vzdrževanja nadzorovan.

14 POLITIKA UPRAVLJANJA VARNOSTNIH INCIDENTOV

14.1 Namen

Dokument predstavlja okvir za upravljanje incidentov. Namen dokumenta je opredeliti postopke, s katerimi družba zagotovi, da se incidenti obvladujejo, oziroma da se odpravijo ali zmanjšajo posledice incidenta. Incidente je potrebno skladno z varnostno politiko identificirati in reševati glede na kritičnost posameznega incidenta.

14.2 Definicija incidenta

Incident predstavlja en ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno delovanje informacijskega sistema oziroma zaupnost, celovitost ali razpoložljivost podatkov, do katerih se dostopa, se jih obdeluje ali hrani.
Incidenti so:

- izguba, uničenje ali zloraba osebnih podatkov in poslovne skrivnosti (podatki v elektronski obliki, papirni dokumenti itd.), ki vpliva na zaupnost, celovitost ali razpoložljivost podatkov;
- namerno ali nenamerno poškodovanje ali zloraba računalniškega informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z zlonamerno programsko opremo, vdori v računalniški informacijski sistem), ki vpliva na razpoložljivost podatkov;
- kraja opreme (strojne ali programske);
- izpad delovanja računalniškega informacijskega sistema (strojna oprema, programska oprema, komunikacije), ki vpliva na razpoložljivost podatkov in storitev;
- kršenje zakonodaje;
- neupoštevanje določil varnostnih politik s strani zaposlenih in tretjih strank.

14.3 Prijava in beleženje incidentov

Vsi zaposleni in uporabniki informacijskega sistema so dolžni prijavljati zaznane incidente pooblaščeni osebi. Prijava incidentov lahko poteka ustno, telefonsko, preko elektronske pošte ali namenskih aplikacij. Pri prijavi incidenta je potrebno navesti:

- kaj se je zgodilo,
- kje je bil zapažen incident,
- kdaj je bil zapažen incident,
- kdo je bil prisoten,
- kakšne so posledice in kakšen vpliv ima incident na delovanje informacijskega sistema oziroma zaupnost, celovitost ali razpoložljivost podatkov, do katerih se dostopa, se jih obdeluje ali hrani.

Pooblaščena oseba vse podatke o prijavljenih incidentih beleži na enem mestu (tabela incidentov) in izvajati aktivnosti odprave oziroma zmanjšanja posledic incidentov.

Vsi incidenti, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov ali poslovne skrivnosti (podatki v elektronski obliki, papirni dokumenti itd.), morajo biti takoj sporočeni vodstvu družbe.

Vsi incidenti, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo strojne ali programske opreme oziroma izpad delovanja računalniškega informacijskega sistema, kar vpliva na razpoložljivost podatkov ali kršenja zakonodaje, morajo biti takoj sporočeni vodstvu družbe. Prav tako morajo biti vsi incidenti sporočeni državnim organom skladno z zahtevami Zakona o informacijski varnosti in v obliki poročil, ki jih državni organi zahtevajo.

Vsi incidenti, ki bi lahko bili posledica oziroma so posledica neupoštevanja določil varnostnih politik, morajo biti sporočeni v rednih poročilih vodstvu družbe.

14.4 Ukrepanje v primeru pojava incidenta

V primeru pojava incidenta se ustrezno ukrepa. Glede na vrsto incidenta se ukrepi delijo na:

- Ukrepanje v primeru izgube, uničenja ali zlorabe podatkov

V primeru incidentov, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov ali poslovne skrivnosti (podatki v elektronski obliki, papirni dokumenti itd.), je potrebno takoj poskrbeti za izvajanje ukrepov za zaščito podatkov. Preostale podatke se mora primerno zaščititi z ustreznimi varnostnimi ukrepi, kar lahko pooblaščena oseba izvede z vsemi strokovno usposobljenimi sodelavci (informatiki, delavci splošnih služb, varnostniki itd.). Revizijske sledi dostopov do izgubljenih, uničenih ali zlorabljenih podatkov se mora preveriti, da se ugotovi, kdo in kdaj je povzročil izgubo, uničenje ali zlorabo podatkov. Na podlagi odgovora vodstva družbe na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident. V primeru zlorabe ključnih krmilnih ali nadzornih sistemov se takoj kontaktira URSIV oziroma SI-CERT, v primeru zlorabe osebnih podatkov pa v roku 72 ur kontaktira Informacijskega pooblaščenca RS.

- Ukrepanje v primeru poškodovanja, zlorabe, izpada delovanja informacijskega sistema ali kraje opreme

V primeru incidentov, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo opreme oziroma izpad delovanja informacijskega sistema, je potrebno poskrbeti za primerno zaščito računalniških informacijskih sredstev (prenos sredstev na varno mesto, omejitev dostopa) oziroma ponovno vzpostavitev delovanja računalniškega informacijskega sistema. Primarne aktivnosti so namenjene vzpostavitvi komunikacijskih povezav in delovanju opreme, namenjene za izvajanje dejavnosti družbe. Na podlagi odgovora vodstva družbe na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident. V primeru zlorabe ključnih krmilnih ali nadzornih sistemov se takoj kontaktira URSIV oziroma SI-CERT.

- Ukrepanje v primeru kršenja zakonodaje

V primeru incidentov, ki predstavljajo direktno kršitev zakonodaje, mora vodstvo družbe takoj obvestiti ustrezne državne institucije (Policija) in v skladu z njihovimi navodili podati vse podatke oziroma predati sredstva, ki so bila uporabljena pri izvajanju prekrška oziroma kaznivega dejanja. Na podlagi odgovora vodstva družbe na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident. V primeru zlorabe ključnih krmilnih ali nadzornih sistemov se takoj kontaktira URSIV oziroma SI-CERT.

- Ukrepanje v primeru neupoštevanja varnostnih politik

V primeru incidentov, ki bi lahko bili posledica oziroma so posledica neupoštevanje določil varnostnih politik, je potrebno zagotoviti primerno zaščito podatkov in informacijskega

sistema ter zabeležiti vse značilnosti incidenta. Na podlagi odgovora vodstva družbe na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

14.5 Pregledovanje in presojanje incidentov

Po zaključenem reševanju incidenta je potrebno oceniti posledice incidenta in ukrepe, ki so bili izvedeni na podlagi incidenta. Oceni se vrsta incidenta, število prizadetih uporabnikov, količina in stopnja zaupnosti izgubljenih, uničenih ali zlorabljenih podatkov, čas trajanja in pogostost pojavljanja.

Pooblaščena oseba ima odgovornost, da ugotavlja, kdo je bil udeležen v posameznem incidentu, v ta namen pa ima pravico do vpogleda v naslednje podatke:

- vsebina elektronske pošte (s privolitvijo osebe, ki ima ta elektronski naslov),
- prometni podatki elektronske pošte,
- prometni podatki dostopa do interneta,
- podatki, ki se nahajajo na računalniški opremi (lokalni disk, USB ključ, strežniška in omrežna infrastruktura itd.) – razen vsebine elektronske pošte in podatkov o dostopih do spletnih strani,
- revizijske sledi dostopa do osebnih podatkov,
- podatki nadzornih mehanizmov (logi brezkontaktnih kartic, videonadzor, biometrija, vpisi v dnevnik dostopov itd.).

Po končanem ugotavljanju odgovornosti za incident pooblaščena oseba pripravi poročilo, ki se posreduje vodstvu družbe. Na podlagi ugotovitev poročila lahko vodstvo družbe sprejme primerne ukrepe, ki lahko izboljšajo stanje varovanja informacij, ter uvede sankcije za osebe, odgovorne za incident.

15 UVELJAVITEV

Te področne politike začnejo veljati in se uporabljajo od objave v Obvestilih. Z dnem objave v Obvestilih prenehajo veljati in se uporabljati Področne politike varovanja informacij (Obvestila 18/24) z dne 13. 12. 2024.

Ljubljana, dne 6. 8. 2025

Glavni direktor
Marjan Eberlinc, univ. dipl. inž. str.

E-žig ustvarjen za:
Marjan Eberlinc
marjan.eberlinc@plinovodi.si

Napredni e-žig s kvalificiranim potrdilom
Imetnik potrdila: mSign
Datum e-žiga: 07.08.2025
Potek veljavnosti potrdila: 04.04.2030

Član poslovodstva
mag. Matija Bitenc, univ. dipl. ekon.

E-žig ustvarjen za:
Matija Bitenc
Matija.Bitenc@plinovodi.si

Napredni e-žig s kvalificiranim potrdilom
Imetnik potrdila: mSign
Datum e-žiga: 11.08.2025
Potek veljavnosti potrdila: 04.04.2030

Vsebine dokumenta "Področne politike varovanja informacij" so nastale v sodelovanju družbe Plinovodi d.o.o. z zunanjim izvajalcem.

16 PRILOGA 1: POSTOPEK IZVAJANJA ANALIZE TVEGANJ

16.1 Namen

Dokument opisuje postopek ocene tveganj, s katerim družba identificira zahteve glede varovanja informacij, ki so osnova za vpeljavo učinkovitega sistema upravljanja varovanja informacij (SUVI).

16.2 Uvod

Tveganja se ocenjuje najmanj enkrat letno oziroma ob spremembah, ki lahko vplivajo na tveganja, kot so spremembe zakonodaje, organiziranosti, poslovnih procesov, informacijskih sredstev, nove grožnje in ranljivosti. Za izvedbo ocene tveganja je potrebno predhodno določiti poslovne procese in njihove zahteve glede varovanja podatkov ter izvesti analizo stanja varovanja informacij.

Postopek ocene tveganj obsega naslednje korake:

- popis informacijskih sredstev (ključni, krmilni in nadzorni informacijski sistemi),
- izvedba analize tveganja,
- obravnavanje tveganj in določitev načrta za znižanje tveganj.

16.3 Popis informacijskih sredstev

Prvi korak pri izvedbi ocene tveganja je popis informacijskih sredstev (ključni, krmilni in nadzorni informacijski sistemi), ki spadajo v obseg ocenjevanja tveganj. Informacijska sredstva imajo ranljivosti, ki jih grožnje lahko izkoristijo in ogrozijo zaupnost, celovitost ali razpoložljivost informacij. Informacijska sredstva popišemo na osnovi poslovnih procesov, ki ta sredstva uporabljajo za podporo svojih poslovnih aktivnosti.
Informacijska sredstva so:

- informacije v elektronski obliki (baze podatkov, datoteke, dokumenti itd.),
- informacije v fizični obliki (papirni dokumenti, slikovni izpisi itd.),
- osebje (administratorji, lastniki informacijskih sredstev, razvijalci, uporabniki itd.),
- strojna oprema (strežniki, mrežna oprema, delovne postaje, prenosni računalniki, periferna oprema itd.),
- programska oprema (operacijski sistemi, aplikacije, komercialna programska oprema itd.),
- prenosni računalniški nosilci podatkov,
- komunikacije,
- infrastruktura,
- prostori.

16.4 Analiza tveganja

Izračun tveganj je postopek, ki na osnovi ocenjene

- verjetnosti groženj in
- stopnje posledic uresničitve groženj,

izračuna tveganja, ki so jim informacijska sredstva izpostavljena. Informacijska sredstva je smiselno združiti v skupine, ki so na enak način izpostavljene grožnjam, saj se tako zmanjša kompleksnost informacij, ki jih moramo obdelati in prikazati. Stopnja posledic uresničitve grožnje je odvisna od zahtev poslovnih procesov. Zato je v večjih družbah zaradi lažje obvladljivosti analizo tveganja smiselno izvesti po poslovnih procesih. V tem primeru je za vsak poslovni proces potrebno ugotoviti, katera informacijska sredstva so potrebna za izvajanje aktivnosti.

- Identifikacija tveganj

Namen procesa identifikacije tveganj je določiti, kaj vse lahko privede do izgube zaupnosti, celovitosti in razpoložljivosti informacijskega sredstva in kakšne bi bile posledice za družbo.

Določi se grožnje, ki bi lahko potencialno škodile informacijskim sredstvom družbe ter ogrozile njihovo zaupnost, razpoložljivost ali celovitost. Informacije o grožnjah se pridobi iz pregleda incidentov, od lastnikov sredstev, uporabnikov sistemov in iz katalogov groženj. Za vsako informacijsko sredstvo in grožnjo se ugotovi možne posledice uresničitve groženje. Ugotovi se vpliv incidentov in možne poslovne in finančne posledice za družbo.

Nato se za vsako informacijsko sredstvo in grožnjo ugotovi ranljivosti, ki jih grožnja lahko izkoristi in se lahko nanašajo na organiziranost, procese in postopke, načine upravljanja, osebje, fizično okolje, konfiguracijo informacijskih sistemov, strojno, programsko in komunikacijsko opremo, odvisnost od zunanjih strank.

Sledi identifikacija obstoječih varnostnih kontrol, s katerimi družba zmanjšuje ranljivosti. Obstoječe kontrole in njihovo učinkovitost ugotovimo s pregledom dokumentacije in dejanskega stanja varovanja, z intervjuji pooblaščene osebe, lastniki, skrbniki in uporabniki informacijskega sistema

- Izračun tveganj

Osnovna predpostavka pri ocenjevanju tveganj je, da se samo ocenjevanje tveganj lahko izvaja nad izbranim obsegom - poslovnimi procesi, organizacijskimi enotami oziroma sredstvi. Vendar pa se moramo zavedati, da sta tudi poslovni proces oziroma organizacijska enota sestavljena iz posameznih sredstev družbe, katere med drugim predstavljajo tudi človeški viri. Zato je smiselno, da je prvi korak pri ocenjevanju tveganj samo definiranje oziroma pregled sredstev, nad katerimi se bo ocenjevanje tveganj izvajalo. Pri tem se moramo zavedati, da sredstva spadajo v posamezne poslovne procese ali/in organizacijske enote, tako da se ocenjevanje tveganj nad poslovnimi procesi ali organizacijskimi enotami izvaja glede na vsa vključena sredstva v posamezen poslovni proces ali organizacijsko enoto. Grožnje, ki pretijo družbi, se zaradi okolja in značilnosti poslovanja razlikujejo od groženj, ki pretijo drugim družbam. Družba mora smiselno definirati grožnje, ki se lahko zgodijo njenemu poslovanju, seveda iz stališča dejavnosti posamezne družbe in zakonodaje ter standardov, ki jih mora družba upoštevati. Za ustrezno in celovito ocenjevanje tveganj je smiselno, če družba pripravi katalog groženj, ki jo zadevajo, kar je razvidno iz okolja družbe in iz sredstev, nad katerimi se bo izvajala ocena tveganja. V obseg ocenjevanja tveganj je potrebno vključiti vse grožnje, ki so povezane s sredstvi in posledično organizacijskimi enotami ali poslovnimi procesi, ki se jih je definiralo v obsegu.

Izračun tveganj po matriki posledic in verjetnosti (Consequence/probability matrix) se lahko izvaja na način, kot ga opredeljuje standard ISO 31010 z uporabo naslednje matrike:

			Posledice					
			Incident ne povzroči škode, ne zaustavi delovanja, ne povzroči izgube ali zlorabe podatkov, ni nevarnosti za zdravje in življenje zaposlenih	Incident povzroči škodo v posamezni organizacijski enoti, izpad delovanja je še sprejemljiv, lahko pride do izgube podatkov, možne lažje poškodbe zaposlenih	Incident povzroči škodo v več organizacijskih enotah, izpad delovanja je še sprejemljiv, lahko pride do izgube ali zlorabe podatkov, verjetne poškodbe zaposlenih	Incident povzroči večjo škodo, izpad delovanja za daljši čas, velika možnost izgube ali zlorabe podatkov, možne večje poškodbe zaposlenih	Incident povzroči veliko škodo družbi, preživetje je oteženo, delovanje ni možno za daljši čas, možna izguba ali zloraba večine podatkov, verjetne težje poškodbe zaposlenih	Incident lahko povzroči konec poslovanja, izpad delovanja za daljši čas, izguba ali zloraba vseh podatkov, verjetnost smrti ali težkih poškodb zaposlenih
			1	2	3	4	5	6
Verjetnost	incident se zgodi večkrat mesečno	E	2	3	4	5	5	5
	incident se zgodi 1x mesečno	D	2	3	3	4	5	5
	incident se zgodi večkrat letno	C	1	2	3	4	4	5
	incident se zgodi 1x letno ali manj pogosto	B	1	2	3	3	4	5
	incident se zgodi 1x na desetletje ali manj pogosto	A	1	1	2	3	4	4

- Obravnavanje tveganj in določitev načrta za znižanje tveganj

Ocenjena tveganja se razvrsti glede na velikost. Vsa tveganja, ki so nesprejemljiva, je potrebno obravnavati. Kriterij za sprejemljivo tveganje je srednje (3), majhno (2) ali zelo majhno (1) tveganje. Za vsa ostala tveganja, ki so višja od sprejemljivega, je na voljo več možnosti:

- določimo in izvedemo ukrepe, ki tveganje znižajo na sprejemljivo vrednost,
- zavestno sprejmemo tveganje, ker ocenjujemo, da bili ukrepi za zmanjšanje predragi oziroma bi motili ali onemogočili normalno izvajanje delovnih procesov,
- tveganjem se izognemo,
- prenesemo tveganje na druge stranke (npr.: zavarovalnice).

Prav tako je po drugi strani priporočljivo uvesti ukrep za zmanjšanje tveganja, ki ni višje od sprejemljivega, če je ukrep cenovno upravičen, kar pomeni, da je povezan z majhnimi stroški ali pa zmanjša tveganje za več različnih groženj.

Oblikuje se načrt za znižanje tveganj, ki vsebuje ukrepe za znižanje tveganj. V načrtu so določene odgovorne osebe za izvedbo ukrepov, ocena stroškov in rok izvedbe. Načrt za znižanje tveganj v obliki tabele ukrepov potrdi vodstvo družbe.

17 PRILOGA 2: NOTRANJA PRESOJA

17.1 Namen

Notranja presoja je mehanizem, ki omogoča pregled nad oceno tveganja, incidenti in ukrepi. Z izvedbo notranje presoje se ugotovi ali je izvajanje dela vseh uporabnikov informacij in informacijskega sistema skladno z sprejetimi pravilniki, navodili, varnostnimi politikami in zakonodajo. Vodstvo družbe dobi po izvedbi notranje presoje poročilo, da vidi kakšno je stanje varovanja informacij in na podlagi ugotovitev sprejme ustrezne ukrepe, ki lahko izboljšajo stanje.

17.2 Izvedba notranje presoje

Notranja presoja se mora izvesti vsaj enkrat letno. Notranjo presojo lahko izvaja pooblaščena oseba, ki je ustrezno usposobljena, oziroma kvalificirani notranji presojevalec SUVI ali preizkušen revizor informacijskih sistemov.

Vhodni podatki za izvedbo notranje presoje

- stanje ukrepov – pregled tabele ukrepov,
- zaznani incidenti – vsi incidenti, ki so se zgodili v času od predhodne notranje presoje,
- pregled sprememb v informacijskem sistemu – spremenjeni procesi, postopki, novi zaposleni, nova organizacijska struktura, nova programska oprema, nova strojna oprema, novi načini komunikacije,
- dokumentacija notranjih opravil – ali je dokumentacija skladna z zakonodajnimi določili in vsemi internimi predpisi.

Dokumentacija za izvedbo notranje presoje

- plan notranje presoje,
- zapisnik notranje presoje.

Izhodni podatki – podatki za vodstveni pregled

- izpolnjen zapisnik notranje presoje,
- priprava na novo oceno tveganja,
- spremembe dokumentacije notranjih pravil.

Izvedba notranje presoje se začne s pregledom tabele ukrepov in trenutnim statusom ukrepov (že izvedeni, v izvedbi, rok že pretečen). V kolikor se ukrepi niso izvedli in je rok že pretečen, se mora ugotavljati, kdo je odgovorna oseba in zakaj do izvedbe ukrepa še ni prišlo. Aktivnosti za izvedbo teh ukrepov se morajo izvesti čim prej, v zapisnik notranje presoje pa zapisati trenutno stanje – opozorilo za vodstvo družbe.

Pregleda se nabor vseh zaznanih incidentov od predhodne notranje presoje in na podlagi ugotovitev pripravi ukrepe, ki bi zmanjšali ali omejili incidente na tako raven, da so sprejemljivi. Aktivnosti za izvedbo teh ukrepov se morajo izvesti čim prej, v zapisnik notranje presoje pa zapisati trenutno stanje – opozorilo za vodstvo družbe.

Pregleda se spremembe, ki so nastale v družbi od predhodne notranje presoje (spremenjeni procesi, postopki, novi zaposleni, nova organizacijska struktura, nova programska oprema, nova strojna oprema, novi načini komunikacije) in se ugotovi, ali so potrebne kakšne spremembe v dokumentaciji notranjih pravil oziroma, ali je potrebno izvesti ukrepe, da zagotovimo primerno vodenje varovanja podatkov. Aktivnosti za izvedbo teh ukrepov se morajo izvesti čim prej, v zapisnik notranje presoje pa je potrebno zapisati trenutno stanje – opozorilo za vodstvo družbe.

Pregleda se dokumentacijo notranjih pravil z namenom ugotovitve skladnosti dokumentov z izvajanjem postopkov v družbi. Vse potrebne spremembe se dokumentira v zapisnik notranje presoje.

Na podlagi informacij notranje presoje se pripravi nova ocena tveganja.

Priloge

- plan notranje presoje,
- zapisnik notranje presoje.

PLAN NOTRANJE PRESOJE	
Referenčna dokumentacija:	Dokumentacija SUVI in SUNP ter NP, veljavna z dne dd. mm. llll
Datum presoje:	dd. mm. llll

Skupina presojevalcev
Ime Priimek, vodja presoje, notranji presojevalec SUVI

Čas	Oddelek / Tema	Varnostne politike	Odgovorna oseba
08.00 09.00	Pregled sprememb v informacijskem sistemu – nova oprema, zaposleni, način sporočanja informacij, način prenosa podatkov		
09.00 10.00	Stanje ukrepov - pregled ocene tveganja, popisa procesov, analiza stanja		
10.00 11.00	Zaznani incidenti – vsi incidenti, ki so se zgodili v času od prejšnje izvedene notranje presoje		
11.00 12.00	Dokumentacija notranjih pravil – skladnost z zakonodajnimi določili in internimi predpisi		
12.00 13.00	Priprava poročila notranje presoje		

ZAPISNIK NOTRANJE PRESOJE	
Referenčna dokumentacija:	Dokumentacija SUVI in SUNP ter NP, veljavna z dne dd. mm. llll
Datum presoje:	dd. mm. llll

Skupina presojevalcev
Ime Priimek, vodja presoje, notranji presojevalec SUVI

VSEBINA

1. UVOD

Namen notranje presoje je bil preveriti učinkovitost vzpostavitve, dokumentiranosti, izvajanja in vzdrževanja notranjih pravil ter vpeljanih ukrepov. Namen notranje presoje ni samo ugotavljanje neskladnosti z zahtevami notranjih pravil ter zakonodaje, temveč ugotavljanje, na kakšen način se lahko v družbi varovanje informacij še izboljša.

Notranja presoja je potekala v skladu z izdelanim planom.

2. TEHNIKA PRESOJE

Za pridobitev potrebnih informacij za presojo skladnosti z zahtevami SUVI in SUNP ter NP so se uporabile naslednje metode:

- razgovor z odgovornim osebjem,
- pregled skladnosti izvajanja dela z zahtevami dokumentacije SUVI in SUNP ter NP,
- pregled zapisov, ki nastanejo pri izvajanju SUVI in SUNP ter NP.

3. UGOTOVITVE

Splošne ugotovitve:

Pregled aktivnosti pooblaščene osebe:

Izvedeno 2x letno preverjanje ali so bile za vse zaposlene in pogodbene sodelavce, ki so prenehali delovno razmerje ali pogodbeno sodelovanje, ukinjene pravice dostopa do informacij, aplikacij in sistemov.	DA / NE	Opombe:
Ugotovitve:		
Izvedeno 2x letno preverjanje, ali so bile za vse zaposlene in pogodbene sodelavce, ki so prenehali delovno razmerje ali pogodbeno sodelovanje, ukinjene pravice dostopa do posameznih območij.	DA / NE	Opombe:
Ugotovitve:		
Izvedeno 2x letno preverjanje, da se podatki dejansko nahajajo na varnostnih kopijah in da podatki niso poškodovani ali uničeni ter opravljeno testiranje s pogodbenimi sodelavci, ali bi bilo v primeru dogodka ali varnostnega incidenta podatke mogoče restavrirati iz varnostnih kopij.	DA / NE	Opombe:
Ugotovitve:		
Dokumentirane vse spremembe strojne in programske opreme v zadnjem letu.	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Dokumentiran razvoj programske opreme v zadnjem letu.	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Dokumentirane vse spremembe v omrežju v zadnjem letu.	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Izveden letni pregled vseh zaznanih incidentov.	DA / NE	Opombe:
Ugotovitve:		
Ustrezno upravljanje in vodenje zapisov pri zaznanih incidentih.	DA / NE	Opombe:
Ugotovitve:		

Preverjanje pogodb in izvajanje dela pogodbenih sodelavcev (tudi upoštevanje SLA določil).	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Izvedeno izobraževanje ob prihodu novega zaposlenega ter za vse zaposlene takrat, ko je to potrebno zaradi sprememb politike varovanja informacij, postopkov ali navodil.	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Ustrezno arhiviranje dokumentov in podatkov	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Ustrezno uničenje dokumentov in podatkov	DA / NE / ni potrebe	Opombe:
Ugotovitve:		
Izveden letni pregled vse podporne infrastrukture (električna energija, hlajenje, komunikacijske povezave) s strani pooblaščenih oseb.	DA / NE / ni potrebe	Opombe:
Ugotovitve:		

4. NESKLADNOSTI

Med notranjo presojo ni bilo ugotovljenih neskladnosti z zahtevami standarda oziroma zakonodaje. Ker se je presoja izvedla po metodi naključnega vzorčenja, ni izključena možnost, da neskladnosti obstajajo.

ALI

Med notranjo presojo so bile ugotovljene neskladnosti z zahtevami standarda oziroma zakonodaje.

Neskladnost 1:

Opis:
OP:
Pravilnik, navodilo, politika:

Neskladnost 2:

Opis:
OP:
Pravilnik, navodilo, politika:

Neskladnost 3:

Opis:
OP:
Pravilnik, navodilo, politika:

5. PRIPOROČILA

Zadeve, v zvezi s katerimi navajamo priporočila, ne predstavljajo neposrednih neskladnosti z zahtevami zakonodaje. Vendar lahko neupoštevanje priporočil privede do neučinkovitosti in s tem do neskladnosti.

Priporočilo 1:

Opis:
OP:
Pravilnik, navodilo, politika:

Priporočilo 2:

Opis:
OP:
Pravilnik, navodilo, politika:

Priporočilo 3:

Opis:
OP:
Pravilnik, navodilo, politika:

6. UGOTOVITVE

STANJE USTREZNO
☐ da / ☐ ne
INCIDENTI (v kolikor stanje ni ustrezno)
POVIŠANA TVEGANJA
☐ da / ☐ ne
UKREPI

7. ZAKLJUČEK

Glede na ugotovitve notranje presoje smo mnenja, da je družba še naprej skladna z zahtevami SUVI in SUNP ter NP, možne pa so še izboljšave.

Na osnovi splošnih ugotovitev in konkretnih ugotovitev te presoje je potrebno izvesti korektivne ukrepe in/ali ustrezne izboljšave. Učinkovitost vpeljanih ukrepov bomo preverili na naslednji notranji presoji.

ALI
Glede na ugotovitve notranje presoje smo mnenja, da družba ni skladna z zahtevami SUVI in SUNP ter NP. Ukrepe je potrebno izvesti v roku 3 mesecev in po izvedbi ukrepov ponoviti notranjo presojo, na kateri se bo preverilo, ali so bili ukrepu ustrezno vpeljani.