INFORMACIJSKA VARNOSTNA POLITIKA ZA ZUNANJE IZVAJALCE

1. Uvod

Dokument »Informacijska varnostna politika za zunanje izvajalce« vsebuje informacije, ki so po klasifikaciji dokumentov opredeljeni kot zaupni. Z informacijami tega dokumenta lahko razpolagajo samo zaposleni in zunanji izvajalci.

Varnost informacijsko-komunikacijskega sistema je vitalna komponenta poslovanja. Zaradi kompleksnosti informacijsko-komunikacijskega sistema so za njegovo obvladovanje potrebna specifična znanja, ki jih je v določenih primerih lažje zagotoviti s pomočjo zunanjih izvajalcev. Namen politike za zunanje izvajanje je zagotavljanje potrebnega nadzora nad delom zunanjih izvajalcev in prepoznavanje tveganj, ki jih vnašajo zunanji izvajalci v poslovne procese.

Dokument je razdeljen na štiri poglavja, v katerih so opredeljeni načini dela, dostop do informacijskih virov, delo zunanjih partnerjev in pogodbene obveznosti.

Dokument se pregleduje letno. V primeru predlaganih sprememb dokumenta varnostni inženir opravi pregled vseh predlaganih sprememb in pripravi končni predlog sprememb dokumenta.

2. Vrste dela

Pred dostopom zunanjih izvajalcev do informacijsko-komunikacijskega sistema se preuči vpliv zunanjega izvajanja na celoten proces in predvsem na zagotavljanje neprekinjenega poslovanja. Analizo vplivov opravi informacijski varnostni inženir. Analiza mora vsebovati tudi ukrepe v primeru nepričakovane prekinitve pogodbenega razmerja z zunanjim izvajalcem.

V primeru, ko varovanje informacij upravlja zunanji izvajalec, se določi način zagotavljanja ustrezne varnosti glede na oceno tveganja (prilagajanje varovanja, prepoznava in obravnava vseh sprememb v zvezi s tveganji).

Vse dejavnosti zunanjih izvajalcev so predmet rednih pregledov z namenom pregleda ustreznosti najema zunanjih izvajalcev in zagotavljanjem ustrezne kakovosti storitve.

2.1 Vzdrževanje – časovno neomejena uporaba

Vzdrževanje obsega vsa operativna dela, ki so potrebna za vsakodnevno delo.

Kontrola 1: Spremljanje in nadzor najema zunanjih izvajalcev.
Za primer časovno neomejenega najema zunanjih izvajalcev se izvaja nadzor na podlagi v naprej dogovorjenih kriterijev in medsebojnih obveznosti, opredeljenih v pogodbi. V primeru nenadne odpovedi pogodbe, so v načrtu neprekinjenega poslovanja opredeljeni alternativni postopki in način delovanja v primeru krajših ali daljših motenj.

2.2 Projekti – časovno zaključeni najem

Projekt obsega razvoj novih produktov ali instalacijo/konfiguracijo informacijskih virov, ki se konča v naprej znanem roku. Vključuje tudi naloge (svetovalne, vzdrževalne), čeprav to po definiciji niso projekti.

Kontrola 2: Spremljanje napredka razvoja po v naprej zastavljenih časovnih mejnikih.
Pri časovno zaključenem najemu zunanjih izvajalcev se izvaja spremljanje napredka razvoja oz. instalacije po v naprej določenih časovnih mejnikih opredeljenih za posamezen projekt.

Kontrola 3: Ukrepanje v primeru odstopanj od vnaprej zastavljenega načrta izvedbe projekta.
Pri vsakem odstopanju od začrtanih rezultatov se ponovno preučijo vsa tveganja in sprejmejo ukrepi za zagotovitev pravočasnega zaključka projekta. V primeru večjih odstopanj lahko na podlagi ocene tveganj zavod prekine pogodbeno razmerje in projekt dokonča z lastnimi viri ali z najemom drugega zunanjega izvajalca. Pri razvoju programske opreme je potrebno za takšne primere v pogodbo vključiti tudi člen, ki opredeljuje lastništvo izvorne programske kode.

3. Dostop do informacijskih sredstev

Odgovorna oseba je dolžna seznaniti zunanjega izvajalca z naslednjimi predpogoji za delo v prostorih zavoda:

- opravljanje dela mora biti najavljeno vsaj 24 ur pred načrtovanim posegom, razen v nujnih primerih, ko poseg zahteva odgovorna oseba,
- ob prijavi posega je potrebno posredovati najmanj naslednje podatke:
  - ime in priimek zunanjega izvajalca,
  - ime podjetja zunanjega izvajalca.

Odgovorna oseba skrbi za ažuren seznam zunanjih izvajalcev. V seznamu mora biti tudi naveden pripadajoč skrbnik posameznega področja.

3.1 Upravičenost dostopa

Kontrola 4: Dostop imajo samo zunanji izvajalci s sklenjeno pogodbo z zavodom.
Pred pričetkom del na zavodu mora imeti zunanji izvajalec sklenjeno pogodbo, in če je potrebno tudi dogovor o varovanju poslovne skrivnosti.

Kontrola 5: Vzpostavljen je proces za redno letno preverjanje upravičenosti dostopa zunanjih izvajalcev.
Redno, letno, se pregleduje dodeljene pravice dostopa uporabnikov do posameznih informacijskih virov ter preveri, kdo ta dostop še potrebuje. Preverjanje se izvaja v sodelovanju z lastnikom informacijskega vira.

Kontrola 6: Dostop zunanjim sodelavcem do internih informacijskih sredstev zavoda mora biti odobren s strani vodstva ter tehnično omejen na najmanjšo možno mero za izvedbo dogovorjenih opravil.
Najmanj enkrat letno se opravi pregled vseh pravic in dostopov za zunanje sodelavce in poslovne partnerje. Če je mogoče, se dostopi zunanjim sodelavcem omogočijo na izrecno zahtevo in z omejenimi termini pristopa.

Vsi nepotrebni dostopi do informacijskih sredstev zavoda se onemogočijo ali trajno izbrišejo.
Pregled izvede skrbnik informacijskega vira in rezultate posreduje odgovorni osebi.

3.2 Dostop do informacijskih virov

Kontrola 7: Vsakemu uporabniku informacijsko-komunikacijskega sistema (zaposleni, poslovni partnerji, zunanji izvajalci, udeleženci izobraževanja) je dodeljena unikatna oznaka.
Za uporabnike skrbi vsaka enota zase. Uporabniki so zavedeni v sisteme po enotah. V kolikor sistemi enot in centra niso povezani, morajo skrbniki posameznih sistemov skrbeti za ažurno stanje podatkov o uporabnikih. Za vzpostavitev oddaljenega dostopa za uporabnike in dostopa do spletnih aplikacij, ki niso v lasti zavoda, se uporabljajo ločeni sistemi za avtentikacijo.

Kontrola 8: Vzpostavljen je proces za dodeljevanje, spremembo in brisanje identifikacije uporabnikov.
Dodeljevanje, sprememba in brisanje identifikacije uporabnikov poteka po določenem postopku.
Dodeljevanje uporabniškega računa:

- Na osnovi pogodbe z zunanjim izvajalcem in podatkov oseb, ki bodo opravljale delo na virih v zavodu, se določijo prijavni parametri za vsako osebo, ki potrebuje dostop.
- Vodja, odgovoren za izvedbo dela, na podlagi poslovne potrebe in v okviru svojih pooblastil podrobneje določi pravice glede na delo, ki ga bo opravljal zunanji izvajalec in jih posreduje skrbniku informacijskega vira.
- Skrbnik informacijskega vira ustrezno nastavi informacijski sistem in seznani vodjo z izvršeno akcijo.

Brisanje uporabniškega računa:

- Vodja, odgovoren za izvedbo dela, posreduje podatke za izbris računa skrbniku informacijsko-komunikacijskega sistema.
- Po prenehanju potrebe po dostopu (prekinitev pogodbe, končanje projekta) se ukinejo pravice dostopa do vseh sistemov.
- Skrbnik onemogoči dostop do uporabniškega računa.

Sprememba uporabniškega računa:

- Vodja, odgovoren za izvedbo dela, posreduje zahteve za spremembe skrbniku.
- Skrbnik ustrezno nastavi informacijsko-komunikacijski sistem in seznani vodjo z izvršeno akcijo.

Kontrola 9: Pooblastitev za skrbniški dostop temelji na poslovni potrebi ter jo določi lastnik informacijskega vira ali sistema.
Dodeljevanje pooblastila za skrbnika se izvaja po v naprej določenem procesu, ki vključuje preverjanje potrebe in podpis dogovora o varovanju poslovne skrivnosti. Odstranitev pooblastil se izvede, če je to možno takoj, najkasneje pa v treh delovnih dneh po odkritju, da ni več poslovnih potreb ali prejemu ustreznega obvestila.

Kontrola 10: Vzpostavljen je proces za redno preverjanje upravičenosti zunanjih uporabnikov, ki jim je dodeljena identifikacija za dostop do produkcijskih sistemov.
Preverjanje upravičenosti dostopa do posameznega informacijskega vira se izvaja za vsak informacijski vir. Za pregled podatkov so odgovorni lastniki informacijskih sredstev.

Kontrola 11: Identiteta zunanjega uporabnika je overjena, preden uporabnik prične z uporabo informacijsko-komunikacijskega sistema ali aplikacije.
Na zavodu obstajajo naslednji načini overjanja:

- aktivni imenik (AD),
- Open Lightweight Directory Access Protocol (LDAP),
- overjanje, ki je izvedeno v posameznih informacijskih rešitvah (npr. OpenVMS).

Avtentikacija uporabnika predstavlja samo začetno preverjanje. Na vsakem informacijskem viru se po osnovni avtentikaciji izvaja avtorizacija dostopa do posameznih delov oz. sklopov v okviru informacijskega vira.

Kontrola 12: Gesla za privilegiran dostop so dostopna samo osebam, ki jih potrebujejo pri svojem delu in so vezana na osebo.
Gesla niso vezana na osebo le v izjemnih primerih. Vsa gesla so shranjena na varnem mestu (zapečatena kuverta) v upravi. Dostop do gesel imajo skrbniki informacijskih virov in komunikacijskega omrežja. Vsak dostop do gesla je zabeležen. Po prenehanju uporabe gesel za privilegiran dostop s strani zunanjih izvajalcev se vsa razkrita gesla ponastavijo na novo vrednost.

Kontrola 13: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete, upoštevajo definirana navodila, če tehnologija to omogoča:

1. Dolžina gesla mora biti vsaj osem znakov.
2. Geslo ne sme vsebovati uporabniškega imena kot dela gesla.
3. Sistem avtomatično zahteva zamenjavo gesla vsakih 180 dni.
4. Geslo se ne sme ponoviti najmanj petkrat ali dve leti.
5. Ob začetni nastavitvi gesla s strani službe informatike se geslo nastavi na poteklo (expired) – uporabnik mora geslo spremeniti ob prvi prijavi.
6. Priporoča se, da geslo vsebuje mešanico črk in ostalih znakov (številke, ločila, posebni znaki).
7. Zahteve za gesla so domena zavoda.

Kontrola 14: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete, so zaščitena:

1. Geslo je šifrirano oz. je zapisana samo zgoščena funkcija gesla, kadar se hrani na informacijsko-komunikacijskem sistemu zavoda. Če šifriranje ni mogoče, je dostop do gesel omejen le na avtorizirane skrbnike sistemov.
2. Gesla ne sme uporabljati več uporabnikov, razen če je zagotovljen nadzor in evidenca (audit) uporabe po uporabnikih.
3. Za ponastavitev gesla je zagotovljen varen proces, ki vključuje preverjanje zahtevka za ponastavitev gesla.
4. Privzeto uporabniško geslo, ki je nastavljeno ob namestitvi operacijskega sistema ali aplikacije, je potrebno spremeniti med ali takoj po namestitvi.
5. Prenašanje nešifriranega gesla preko interneta, javnih omrežij ali brezžičnih omrežij ni dovoljeno.

Kontrola 15: Vse nedejavne seje se po določenem času neaktivnosti prekinejo.
Nedejavne seje se po določenem času, ki ga določi skrbnik vira, prekinejo. Uporabnik se mora potem ponovno prijaviti.

Kontrola 16: Dobavitelj ali služba informatike mora poskrbeti za varnostno nastavitev uporabniških virov, ki dovoli dostop le pooblaščenim uporabnikom, potrjenim s strani upravljavca informacijskega vira. Pred prehodom v produkcijsko okolje je potrebno onemogočiti vsa privzeta uporabniška imena

in spremeniti privzeta gesla na vseh sistemih. Dostop do informacijskega sistema je omogočen samo uporabnikom, ki dostop potrebujejo za opravljanje svojega dela.

4. Upravljanje z informacijskimi sredstvi

Kontrola 17: Zunanji izvajalec lahko dostopa v omrežje zavoda samo s parametri, ki mu jih določi odgovorna oseba.
Za dostop do omrežja oz. sredstev zavoda je potrebno uporabljati samo programsko opremo, ki jo predpiše in potrdi odgovorna oseba za informacijsko varnost. Odgovorna oseba zavoda preda vse potrebne parametre za dostop na omrežje in/ali informacijska sredstva zunanjemu izvajalcu po podpisu pogodbe. Vse tehnične probleme rešuje zunanji izvajalec s skrbnikom sistema ali odgovorno osebo.

Kontrola 18: Zunanji izvajalec mora za dostop do omrežja zavoda uporabiti le varnostno pregledano in licencirano informacijsko opremo.
Skrbnik informacijsko-komunikacijskega sistema zavoda ima pravico varnostno pregledati informacijsko opremo zunanjega izvajalca. V primeru odstopanj od standardov zaščite podjetja ima skrbnik pravico prekiniti (odvzeti) dostop zunanjemu izvajalcu do omrežja in/ali sistemov zavoda.

Kontrola 19: Zunanji izvajalec lahko opravlja dela v za to odobrenih prostorih. V primeru, da zunanji izvajalec opravlja delo v prostorih zavoda, se lahko priklopi na omrežje in opravlja svoje delo samo v prostorih, ki mu jih predpiše odgovorna oseba.

Kontrola 20: Zunanji izvajalec lahko opravlja dela samo ob prisotnosti zaposlenega na zavodu.
Delo v zavarovanih prostorih (npr. prostor s strežniki) in na kritičnih sistemih lahko opravlja zunanji izvajalec samo ob prisotnosti zaposlenega v zavodu.

Kontrola 21: Dostop zunanjega izvajalca za delo na daljavo se odobri za vsak poseg posebej. Dostop potrdi odgovorna oseba, ki poskrbi, da se zunanjemu izvajalcu omogoči dostop do omrežja in/ali informacijskega sredstva zavoda s predpisano programsko opremo in ustreznimi parametri. Vsak dostop za delo na daljavo je časovno omejen na posamezen poseg in se ne sme izvajati zunaj razpona delovnega časa, če to ni posebej odobreno.

Kontrola 22: Zunanji izvajalci morajo uporabljati predpisano programsko opremo za vzpostavitev povezave do omrežja in/ali informacijska sredstva zavoda.
Dostop iz delovnih postaj izven omrežja zavoda je izveden z vzpostavitvijo varne povezave s predpisanim odjemalcem.

Kontrola 23: Delo preko zunanje povezave je možno samo za v naprej dogovorjene posege.

Kontrola 24: Zunanji razvijalci programske opreme morajo v okviru razvoja opraviti varnostno testiranje produkta.
Testne parametre za varnostno testiranje določi vodja projekta v sodelovanju z odgovorno osebo za informacijsko varnost. Rezultate varnostnega testiranja je potrebno predložiti takoj po opravljanjem testiranju, vendar najkasneje pred implementacijo programske opreme.

Kontrola 25: Zunanji razvijalci programske opreme morajo v okviru priprave končne verzije produkta izvesti tudi varnostno preverjanje (preverjanje prisotnosti škodljive programske opreme).

V implementaciji te zahteve mora biti vključeno naslednje:
- Pred prenosom aplikacije v produkcijsko okolje mora biti aplikacija varnostno preverjena.
- Varnostno preverjanje mora biti izvedeno tudi za nove verzije že vpeljanih aplikacij.

Kontrola 26: Nadzorne zapise je potrebno kreirati za vse uspešne in neuspešne poskuse dostopa do omrežja zavoda iz zunanjih lokacij.
Vsi zapisi morajo biti shranjeni na ločenem sistemu v omrežju zavoda. Izjeme v nadzornih zapisih niso dovoljene. Zapise je potrebno tedensko (avtomatsko ali ročno) preveriti zaradi odkrivanja sistematičnih napadov.

Kontrola 27: Podatki o aktivnosti morajo vsebovati vsaj naslednje parametre: datum in čas, tip poskusa dostopa, identifikacija uporabnika.
Različni informacijski viri hranijo informacije v različnih formatih z različnimi parametri. Vsi informacijski sistemi hranijo najmanj zgoraj naštete parametre.

Kontrola 28: Po prenehanju dela mora zunanji izvajalec odgovorni osebi zavoda predati vse pridobljeno gradivo zavoda, ki ga je pridobil v času pogodbene aktivnosti v zavodu.
Zunanji izvajalec mora vse pridobljeno gradivo, ki ga je dobil v okviru izvajanja pogodbenih aktivnosti od zaposlenih v zavodu, predati odgovorni osebi zavoda pred zaključkom aktivnosti.

5. Priporočena določila pogodbe z zunanjim izvajalcem

Pred dostopom do informacijskih virov oz. omrežja zavoda je potrebno skleniti pogodbo oziroma ustrezen pisni dogovor z zunanjim izvajalcem.

V proces priprave pogodbe je vključena odgovorna oseba zavoda in odgovorna oseba za informacijsko varnost, ki pomaga pri identifikaciji tveganj, načrtovanju ustreznih kontrol, sistema poročanja in kasneje nadziranju izvrševanja pogodbenih obveznosti.

V pogodbi je podan način dela in dostopa do omrežja in storitev, ki so predmet zunanjega izvajanja ali vzdrževanja. Podrobni podatki o dostopu vsebujejo ime in priimek osebe, zaposlene v podjetju zunanjega izvajalca, izjavo o tajnosti in nerazkritju podatkov ter informacij, do katerih ima dostop med svojim delom.

Pogodba med zunanjim izvajalcem in zavodom vsebuje:
- varnostne odgovornosti zunanjega izvajalca in njegovih podizvajalcev,
- načine vzdrževanja in testiranja opreme, ki je predmet pogodbe z zunanjimi izvajalci z namenom, da se ohrani zaupnost in celovitost informacij,
- postopke in varnostne mehanizme, ki se bodo upoštevali pri dostopu zunanjega izvajalca,
- način zagotavljanja varovanja opreme in podatkov, ki se vnašajo ali iznašajo iz zavoda,
- pravice pooblaščenih delavcev zavoda do stalnega nadzora izvajanja del zunanjega izvajalca,
- zagotavljanje skladnosti delovanja zunanjega izvajalca z veljavno zakonodajo in drugimi predpisi,
- merila, na podlagi katerih lahko naročnik (zavod) in zunanji izvajalec ocenita ustreznost kakovosti storitve.

Določila v pogodbi med zunanjim izvajalcem in zavodom se pred podpisom ustrezno uskladijo tako, da zahteve v pogodbi ne vplivajo na oslabitev:

- izvajanja poslovnih dejavnosti,
- procesa upravljanja s tveganji,
- sistema notranjih kontrol.

To velja še posebej v primeru, če pogodbo pripravi zunanji izvajalec. Pogodbene obveznosti zunanjih izvajalcev so določene glede na zahteve, ki izhajajo iz zagotavljanja ustrezne kakovosti storitev in identificiranimi tveganji, ki se nanašajo na storitev oz. poslovno dejavnost, ki jo izvaja zunanji izvajalec za zavod.

Za zagotovitev ustrezne ravni kakovosti storitve vsebuje pogodba o ravni kakovosti storitev kvantitativna in/ali kvalitativna merila, na podlagi katerih lahko zunanji izvajalec in zavod ocenita ustreznost kakovosti storitve.
Pred vsako uporabo imena zavoda v kakršnekoli namene (npr. marketing, reference) mora zunanji izvajalec pridobiti soglasje odgovorne osebe na zavodu.

5.1 Kontrole v pogodbi z zunanjimi izvajalci:

Kontrola 1: Dela lahko opravljajo samo zunanji izvajalci s sklenjeno pogodbo z zavodom. Podjetje zunanjega izvajalca določi osebe, ki bodo opravljale delo. Vsako spremembo oseb, ki potrebujejo dostop do virov zavoda, je potrebno sporočiti vnaprej.

Kontrola 2: Vsi posegi se opravljajo praviloma samo v testnem ali razvojnem okolju. V izjemnih primerih je možen poseg tudi neposredno na produkcijsko okolje. Vsak poseg v produkcijsko okolje mora biti predhodno odobren s strani odgovorne osebe in ustrezno nadzorovan.

Kontrola 3: Zunanji izvajalec mora upoštevati vse interno predpisane postopke in varnostne mehanizme pri delu z informacijskimi viri zavoda.

Kontrola 4: Opravljanje dela mora biti najavljeno vsaj 24 ur pred posegom, razen v nujnih primerih, ko poseg zahteva odgovorna oseba zavoda.

Kontrola 5: Ob prijavi posega mora zunanji izvajalec posredovati naslednje podatke:

- ime in priimek osebe, ki bo opravljala poseg,
- ime podjetja zunanjega izvajalca,
- namen oz. opis posega.

Kontrola 6: Vsi posegi zunanjih izvajalcev morajo ohraniti zaupnost, razpoložljivost in celovitost obstoječih informacij.

Kontrola 7: Odgovorna oseba zavoda ima pravico stalnega nadzora izvajanja del zunanjega izvajalca.

Kontrola 8: Zunanji izvajalec lahko opravlja dela v za to odobrenih prostorih ali po posebni odobritvi na daljavo. Pri delu na daljavo mora upoštevati vse predpisane varnostne mehanizme.

Kontrola 9: Zunanji izvajalec lahko opravlja dela, kjer je potreben fizični dostop do informacijskih virov samo ob prisotnosti odgovorne osebe zavoda.
Kontrola 10: Dostop zunanjega izvajalca za delo na daljavo se odobri za vsak poseg posebej.

Kontrola 11: Zunanji izvajalec se lahko priklopi na omrežje samo s parametri, ki mu jih določi/ sporoči odgovorna oseba zavoda.

Kontrola 12: Zunanji izvajalci morajo uporabljati predpisano programsko opremo in način dela za vzpostavitev povezave do omrežja zavoda.

Kontrola 13: Delo preko stalno vzpostavljene zunanje povezave je možno samo za v naprej dogovorjene posege.

Kontrola 14: Vsak dlje trajajoči projekt/poseg se spremlja z namenom spremljanja napredka razvoja po v naprej zastavljenih časovnih mejnikih.

Kontrola 15: Vsak poseg je zabeležen z namenom spremljanja, ocenitve kakovosti in nadzora uporabe zunanjih izvajalcev.

Kontrola 16: Po končanem posegu mora zunanji izvajalec pripraviti poročilo o poteku in uspešnosti posega. Poročilo mora posredovati odgovorni osebi zavoda.

Kontrola 17: Po končanem posegu mora zunanji izvajalec predati vse pridobljene informacije v okviru dela odgovorni osebi zavoda.

Kontrola 18: Poseg ali aktivnost se zaključi po sprejemu in potrditvi poročila o opravljenem posegu. Poročilo potrdi odgovorna oseba na zavodu.

6. Prehodne in končne določbe

Skrbniki informacijsko-komunikacijske tehnologije so dolžni v roku 18 mesecev po sprejemu varnostne politike zagotoviti spoštovanje pravil iz tega dokumenta.

Informacijska varnostna politika za zunanje izvajalce velja za vse zunanje izvajalce zavoda.

Vsaka kršitev navodil v dokumentu se obravnava kot kršitev pogodbenih obveznosti.

Dokument prične veljati teden dni po objavi na spletnih straneh in oglasnih deskah zavoda.

Ravnatelj/ica/direktor/ica

Helena Posega Dolenc

Kraj in datum: Postojna, 1. september 2022