KROVNA INFORMACIJSKA VARNOSTNA POLITIKA

1. Uvod

Dokument »Krovna informacijska varnostna politika« vsebuje javne informacije, ki po klasifikaciji dokumentov ne potrebujejo posebne oznake. Z informacijami tega dokumenta morajo biti seznanjeni vsi uporabniki informacijsko-komunikacijskega sistema zavoda.

Osnovna naloga informacijsko-komunikacijskega sistema zavoda je zagotavljanje celovite, prilagodljive in učinkovite informacijske podpore.

Informacijsko-komunikacijski sistem skrbi za razvejano infrastrukturo, ki omogoča izvajanje računalniških, informacijskih, komunikacijskih in drugih storitev ter zagotavlja dostop do virov, potrebnih za nemoten potek izobraževanja, raziskovanja in operativnega dela. Med pomembnejšimi nalogami so:

- načrtovanje in upravljanje osnovne informacijske infrastrukture osrednjega informacijsko-komunikacijskega omrežja in osrednjih strežnikov informacijsko-komunikacijskega sistema,
- storitve za zagotavljanje dostopa do omrežja in njegovih storitev (dostop, naslovi IP, e-pošta, spletni strežniki),
- vzdrževanje in razvoj aplikacij informacijsko-komunikacijskega sistema,
- administracija računalniške in komunikacijske opreme,
- delovanje centra za pomoč uporabnikom - zaposlenim v okviru posameznih služb,
- distribucija programske opreme,
- varovanje in zaščita podatkov,
- izobraževanje uporabnikov.

Ob zavedanju pomena nemotenega delovanja informacijsko-komunikacijskega sistema, za učinkovito podporo delovanja vseh storitev, zavod sprejema Informacijsko varnostno politiko (IVP), kakor tudi njeno izvajanje. Dosledno izvajanje informacijske varnostne politike zagotavlja učinkovito obvladovanje informacijske varnosti:

- **Zaupnost**: pomeni zaščito občutljivih poslovnih informacij pred nepooblaščenim dostopom ali protipravnim prestrezanjem. Zaupnost zagotavlja, da je informacija dostopna samo tistim, ki imajo ustrezna pooblastila. V primeru izpada drugih varnostnih mehanizmov (npr. ukraden prenosni računalnik, ukradeni podatki s strežnika) nam zaupnost zagotavlja, da so vsi podatki neuporabni - zapisani v nerazumljivi/neuporabni obliki.

- **Celovitost**: obravnava zagotavljanje pravilnosti ter celovitost informacij in programske opreme. Kontrola celovitosti se uporablja za zaščito podatkov in sistemov pred nepooblaščeno spremembo. Celovitost olajša ugotavljanje sprememb ter preprečuje, da bi spremenjeno kopijo obravnavali kot original.

- **Razpoložljivost**: zagotavlja, da so informacije in poslovno pomembne storitve, aplikacije in procesi na voljo pooblaščenim uporabnikom, ko jih le ti potrebujejo.

Vsi zaposleni in uporabniki storitev so z Informacijsko varnostno politiko seznanjeni in so jo dolžni razumeti in spoštovati.

Vsaka kršitev določil Informacijske varnostne politike predstavlja kršitev delovnih ali pogodbenih oziroma drugih obveznosti in se sankcionira po veljavnih internih pravilnikih za zaposlene. Dokument se pregleduje letno. V primeru predlaganih sprememb dokumenta varnostni inženir opravi pregled vseh predlaganih sprememb in pripravi končni predlog sprememb dokumenta.

2. Krovna informacijska varnostna politika

2.1 Cilj informacijske varnosti

Cilj informacijske varnosti je zagotoviti nemoteno in varno poslovanje in zmanjšati škodo s preprečitvijo in zmanjšanjem posledic neželenih informacijskih varnostnih dogodkov.

2.2 Informacijska varnostna politika

Namen varnostne politike je zaščita informacijskih sredstev in virov pred vsemi nevarnostmi, notranjimi ali zunanjimi, namernimi ali nenamernimi. Varnostna politika predstavlja na enem mestu zbrana navodila ter standarde za zagotavljanje in upravljanje z informacijsko varnostjo za vse uporabnike informacijskega sistema.

Informacijska varnostna politika obsega:

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij,
- varovanje informacij pred nepooblaščenim dostopom, razkritjem, spremembo ali uničenjem,
- zagotavljanje izobraževanja o informacijski varnosti vsem zaposlenim,
- seznanjanje s pravili varne uporabe za vse uporabnike informacijske infrastrukture,
- obvladovanje vseh varnostnih incidentov ter ustrezno ukrepanje,
- izpolnjevanje usklajenosti z zakoni in predpisi.

Vsi, ki imajo dostop do informacijsko-komunikacijskega sistema, morajo izpolnjevati zahteve informacijske varnostne politike.

Odgovorna oseba, ki koordinira delo z zunanjimi izvajalci, je zadolžena, da se zunanji izvajalec seznani z varnostno politiko in upošteva njena določila. Zunanji izvajalec mora pred pričetkom del podpisati izjavo o seznanitvi in izpolnjevanju določil informacijske varnostne politike.

2.3 Organizacija upravljanja informacijske varnosti

Upravljanje in obvladovanje informacijske varnosti obsega:

- razumevanje strateških ciljev in smernic razvoja tehnologije za oblikovanje dolgoročne strategije informacijske varnosti,
- definicijo, vzpostavitev, vzdrževanje in izvajanje informacijske varnostne politike,
- pridobitev podpore informacijske varnosti,
- razvoj in vzdrževanje visokega nivoja informacijske varnosti,
- spremljanje in upoštevanje zakonodaje na področju informacijske varnosti,
- zagotavljanje varnostnega svetovanja,
- zagotavljanje izobraževanja in seznanjanja o informacijski varnosti vsem uporabnikom informacijskih sredstev,
- obveščanje vodstva o varnostnih vprašanjih in z njimi povezanimi tveganji.

2.3.1 Vodstvo

Vodstvo mora zagotoviti, da zaposleni izpolnjujejo zahteve informacijske varnostne politike. Odgovorno je za zavrnitev neupravičenih ali nepotrebnih zahtev po dostopu do informacijskih virov ter za zagotavljanje ukinitve dostopa do informacijskih virov, ko ga zaposleni ne potrebuje več.
Vodstvo je odgovorno za učinkovito upravljanje z informacijsko varnostjo. V ta namen izvaja vodstvene preglede učinkovitosti sistema za upravljanje z varnostjo, ki obsegajo preglede:

- rezultatov revizij in pregledov sistema,
- poročila ocene tveganja in identificiranih groženj,
- poročila o spremembah, ki lahko vplivajo na informacijsko varnost,
- predlogov za izboljšave.

V okviru svojega dela ima vodstvo tudi naslednje zadolžitve:

- potrjuje strateške smernice za informacijsko varnost,
- potrjuje dokumente informacijske varnostne politike,
- pomaga pri uvajanju večjih projektov informacijske varnosti,
- nadzira večje spremembe pri izpostavljenosti informacijskih sredstev varnostnim grožnjam,
- nadzira in ocenjuje varnostno učinkovitost in zmogljivost.

2.3.2 Odgovorna oseba za informacijsko varnost

Odgovorna oseba za informacijsko varnost je zadolžena za učinkovito izvajanje informacijske varnosti. Naloge odgovorne osebe za informacijsko varnost so:

- poročanje vodstvu o vseh zadevah, ki so povezane z informacijsko varnostjo,
- svetovanje o vseh področjih, ki so povezana z informacijsko varnostjo,
- pregled in posodabljanje kataloga tveganj,
- pregled in posodabljanje kataloga sprememb v IKT infrastrukturi in kataloga varnostnih incidentov,
- razvoj varnostne politike in nadzorstev,
- nadzor izvajanja varnostne politike in nadzorstev.

2.3.3 Lastnik informacijskega sredstva

Lastnik informacijskega sredstva je odgovoren za nadzor, razvoj, vzdrževanje in varovanje informacijskega sredstva. Naloge lastnika informacijskega sredstva so:

- potrjevanje upravičenosti dostopa za posamezne uporabnike ob zahtevi za dostop,
- pregled varnostnih dogodkov v dnevniških zapisih in ukrepanje v primeru zaznanih nepravilnosti,
- pregled uporabnikov s pravicami za dostop do informacijskega vira (enkrat letno),
- pregled uporabnikov s posebnimi (administrativnimi) pravicami dostopa v rednih časovnih intervalih (vsakih 6 mesecev).

2.3.4 Skrbnik informacijskega vira in komunikacijske infrastrukture

Skrbnik je zadolžen za vzpostavitev delovanja, nastavitve in vzdrževanje informacijskih virov in komunikacijske infrastrukture. Naloge skrbnika so:

- preverjanje delovanja informacijskega vira in komunikacijske infrastrukture,
- vpeljava in vzdrževanje informacijskih rešitev z namenom zagotavljanja nemotenega delovanja informacijskega vira ali komunikacijske infrastrukture,

- implementacija varnostnih nastavitev za informacijski vir ali komunikacijsko infrastrukturo,
- odprava napak v delovanju in raziskovanje vzrokov za motnje v delovanju,
- stalno izobraževanje z namenom osveževanja znanja na področju dela, ki ga opravlja skrbnik.

2.3.6 Uporabniki informacijsko-komunikacijskega sistema

Vsi zaposleni, udeleženci izobraževanja in drugi uporabniki informacijsko-komunikacijskega sistema, vključno z zunanjimi izvajalci, morajo upoštevati informacijsko varnostno politiko, ki je zapisana v dokumentu »Informacijska varnostna politika za uporabnike«. Informacijska varnostna politika za zunanje izvajalce je zapisana v dokumentu »Informacijska varnostna politika za zunanje izvajalce«.

2.4 Upravljanje informacijskih virov

Razvoj, uvajanje in vzdrževanje informacijskih virov in sredstev mora potekati v skladu z varnostnimi zahtevami, definiranimi v dokumentu »Informacijska varnostna politika za področje informacijsko-komunikacijske tehnologije (IKT)«.

3. Prehodne in končne določbe

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

Informacijska varnostna politika za zaposlene velja za vse uporabnike informacijsko-komunikacijskega sistema.

Vsaka kršitev navodil v dokumentu se obravnava kot kršitev delovnih in 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