REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

POLITIKA O VARNOSTI OMREŽNIH IN INFORMACIJSKIH SISTEMOV – vzorčna dokumentacija

Različica:	1.0
Datum veljavnosti:	
Avtor:	
Odobril:	

November 2025

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Politika o varnosti omrežnih in informacijskih sistemov« iz 1. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1). Dokument je generičen in je namenjen kot pomoč pri doseganju skladnosti predvsem malim in srednje velikim organizacijam v Republiki Sloveniji (do približno 200 uporabnikov oziroma naprav), ki morajo izpolnjevati zahteve iz ZInfV-1[1].

V dokumentu so generično navedene najbolj relevantne in pogosto uporabljene splošne in konkretne politike, ki se uporabljajo za zagotavljanje varnosti omrežnih in informacijskih sistemov, ki pa niso nujno relevantne za vsakega posameznega zavezanca enako.

Dokument ni univerzalna rešitev, temveč izhodiščni okvir, ki ga mora vsaka organizacija obvezno prilagoditi svojemu dejanskemu stanju informacijsko-komunikacijske infrastrukture, posebnostim sektorja (npr. zdravstvo, finance, energetika, javna uprava), obsegu poslovanja, storitvam zunanjih ponudnikov storitev ter rezultatom izvedene analize obvladovanja tveganj (register tveganj, ugotovljene ravni (preostalega) tveganja in sprejeti/predlagani ukrepi za njihovo obvladovanje).

Organizacija tako na podlagi rezultatov zadnje izvedene analize obvladovanja tveganj določi, katere splošne varnostne ukrepe in kontrole bo predpisala s krovno varnostno politiko in katere posebne varnostne ukrepe ter kontrole bo predpisala s področnimi varnostnimi politikami.

Dokument mora biti tako usklajen z rezultati izvedene zadnje analize obvladovanja tveganj na področju informacijske varnosti in načrtom varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost.

Po ustrezni prilagoditvi oziroma dopolnitvi dokument potrdi vodstvo organizacije in ga pregleda vsaj enkrat letno ali ob vsakem pomembnem incidentu, pomembnih spremembah v informacijsko-komunikacijski infrastrukturi, pomembnih spremembah organiziranosti ali procesov ali v primeru spremembe pomembnih tveganj.

<u>*Uporabljeni viri*</u>*:*

- *Zakon o informacijski varnosti (Uradni list RS, št. 40/25);*
- *Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024, o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022;*
- *Standard ISO/IEC 27002:2022;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *SOC 2 - System and Organization Controls 2 (Trust Services Criteria);*
- *Technical Implementation Guidance on Cybersecurity Risk Management Measures, ENISA, junij 2025.*[2]

[1] Zavezanci iz ZInfV-1, ki so ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnega centra, ponudniki omrežij za dostavo vsebin, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja, morajo pri pripravi tega dokumenta upoštevati določbe Izvedbene uredbe Komisije (EU) št. 2024/2690, z dne 17. oktobra 2024.

2 (https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

KAZALO

1. Uvod

Politika informacijske varnosti (v nadaljevanju - politika) je ključen element upravljanja tveganj in zaščite informacijskih sredstev vsake organizacije. Vsi zaposleni in pogodbeni partnerji so se dolžni s to politiko seznaniti in so dolžni politiko spoštovati in jo dosledno izvajati. Seznanjenost z politiko mora biti dokazljiva (npr. s podpisom ali na drug dokumentiran način).

Ta dokument določa celovito politiko informacijske varnosti organizacije, ki je usklajena s strateškimi cilji organizacije in z veljavnimi predpisi s področja informacijske in kibernetske varnosti ter sledi dobrim praksam na tem področju.

Politika zagotavlja okvir za varno upravljanje sredstev ter določa vloge, odgovornosti in postopke za njihovo zaščito. Sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za organizacijo in omogoča ustvarjanje, obdelavo, hrambo ali prenos informacij ali izvedbo storitve, zaradi katere je organizacija določena kot zavezanec.

Politiko odobri vodstvo organizacije. Pregleda in posodobi jo najmanj enkrat letno oziroma ob večjih spremembah. Odobritev, pregled in posodobitev politike morajo biti dokumentirane.

Vsako odstopanje od zahtev te politike obravnava vodstvo, ki lahko izrecno določi izjeme oziroma odstopanja od zahtev te politike. Vse izjeme se dokumentirajo z utemeljitvijo, časovno omejitvijo in datumom naslednjega pregleda v seznamu izjem, ki vsebuje najmanj naslednje podatke:

- Identifikator izjeme;
- Naziv izjeme;
- Opis izjeme;
- Utemeljitev (kontrole, ki pripomorejo k obvladovanju tveganj povezanih z izjemo);
- Datum prve odobritve izjeme in
- Identifikator sklepa ali druge formalne odobritve vodstva organizacije za izjemo.

Ukrepi oziroma zahteve politike temeljijo na evropskih in mednarodnih standardih (ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319401, CEN/TS 18026:2024, NIST-CSF, SOC2) in so prilagojeni velikosti organizacije, naravi dejavnosti in stopnji izpostavljenosti tveganjem.

1.1 Vloge, odgovornosti in pooblastila

Za izvajanje politike informacijske varnosti so v podjetju določene naslednje ključne vloge in njihove odgovornosti (podrobna delitev glob in stopenj odgovornosti je razvidna iz Priloge 1 – matrika ZOPS)[3], ki so razporejene tako, da se zagotavlja načelo ločevanja dolžnosti ter preprečuje možnost zlorabe pooblastil:

- **Vodstvo organizacije** je odgovorno za:
  - strateško usmerjanje organizacije;
  - zagotavljanje virov, vključno s kadrovskimi, finančnimi in procesnimi viri ter orodja, sredstva in tehnologije za zagotavljanje in izboljševanje informacijske varnost v organizaciji;
  - sprejem in potrjevanje krovne politike in področnih politik informacijske varnosti;
  - upravljanje tveganj, vključno z odobritvijo ukrepov za obvladovanje tveganj ter nadzor nad njimi;
  - izvedbo lastnega usposabljanja na področju obvladovanja tveganj;
  - usposabljanja skrbnikov informacijsko-komunikacijskih sistemov;
  - usposabljanja zaposlenih na področju informacijske in kibernetske varnosti in

[3] ZOPS (ang. *RACI Matrix*) - Zadolžen, Odgovoren, Posvetovan, Sporočeno.

- nadzor nad vodjo informacijske varnosti (če je imenovan).

– **Vodja informacijske varnosti (CISO)**[4] **je odgovoren za:**
  - vzpostavitev, upravljanje in spremljanje izvajanja politike o varnosti omrežij in informacijskih sistemov;
  - svetovanje ter poročanje vodstvu in
  - usklajevanje odzivov na incidente.

– **Skrbniki informacijskih sistemov in omrežij:**
  - imajo privilegiran dostop do omrežij in informacijskih sistemov;
  - izvajajo tehnične ukrepe za zaščito informacijskih sistemov;
  - spremljajo dnevniške zapise;
  - izvajajo popravke in
  - izvajajo druga strokovno-tehnična opravila.

– **Lastniki informacijskih sredstev** so odgovorni za**:**
  - opredelitev zahtev glede zaupnosti, razpoložljivosti, avtentičnosti in celovitosti posameznih sredstev.

– **Zaposleni in pogodbeni izvajalci** so odgovorni za**:**
  - spoštovanje določb te politike, poročanje o incidentih in varno ravnanje s podatki.

– **Vodje organizacijskih enot (oddelkov, sektorjev, …):**
  - skrbijo za izvajanje politik na ravni svojih enot in za ozaveščanje zaposlenih.

– **Pooblaščene osebe za stike z dobavitelji (skrbniki pogodb)** so odgovorne za**:**
  - varnostno presojo in pogodbeno ureditev razmerij z dobavitelji.

– **Kontaktna oseba za informacijsko varnost in njen namestnik:**
  - sta vezni člen med organizacijo in pristojnim nacionalnim organom (URSIV);
  - sporočata obvezne podatke organizacije iz 8. člena ZInfV-1[5] ter spremembe teh podatkov in
  - poročata o morebitnih incidentih.

Vsaka vloga mora biti dokumentirana v okviru matrike ZOPS ali drugega organizacijskega dokumenta, pri tem se mora upoštevati ločevanje nasprotujočih si nalog in področij odgovornosti.

1.2 Namen in obseg

Politika je skladna s strategijo in kontekstom organizacije ter upošteva analizo vpliva na poslovanje (ang. *Business Impact Analysis - BIA*). Določa postopke in načine varovanja informacij in informacijskih sredstev za zagotavljanje zaupnosti, celovitosti, razpoložljivosti in avtentičnosti informacij ter skladnosti z ZInfV-1. Politika velja za vse zaposlene, pogodbenike in zunanje sodelavce organizacije ter obsega vse informacijske sisteme, sredstva, naprave in podatke, ki jih organizacija obdeluje.

[4] CISO ni obvezna vloga po ZInfV-1; če je imenovan, lahko vodstvo nanj pod določenimi pogoji prenese nekatere naloge in odgovornosti.
[5] Zakon o informacijski varnosti (Uradni list RS, št. 40/25).

Neupoštevanje določb informacijske varnostne politike predstavlja kršitev delovnih obveznosti in se lahko sankcionira v skladu z delovnopravnimi predpisi.

Politika ne velja za…. [NAVEDBA IS, SREDSTEV, PARTNERJEV, PODATKOV… , KI SO IZKLJUČENA IZ OBSEGA].

1.3 Načela informacijske varnosti

Zaupnost (Z):

- Dostop do sredstev, naprav in podatkov je dovoljen samo pooblaščenim uporabnikom, procesom ali sistemom.
- Pravice za dostop se dodeljujejo po načelu najmanjših pravic (ang. *least privilege*) in ne v večjem obsegu, kot je nujno za izvedbo naloge, procesa ali storitve (ang. *need-to-know*).
- Podatki se klasificirajo glede na občutljivost, pri prenosu in hrambi se uporablja močne šifrirne algoritme s postopnim prehodom na post-kvantne algoritme.
- Dostop zunanjih izvajalcev do naprav, sistemov ali podatkov organizacije mora biti določen v pogodbah, ki vsebujejo tudi klavzulo o nerazkritju (ang. *NDA*).
- Omrežja in naprave morajo biti ločene na način, da preprečujejo nenameren ali nameren dostop iz drugih (nepooblaščenih) delov omrežja, dostop iz medmrežja do notranjih sistemov in delov omrežja pa mora biti urejen na način, da je dostop čim bolj omejen.

Celovitost (C):

- Vsi deležniki morajo skrbeti, da podatki niso nepooblaščeno spreminjani ali izbrisani.
- Spremembe v sistemih morajo biti nadzorovane, odobrene in morajo zagotavljati revizijsko sled ter omogočati preverjanje pristnosti.
- Uporabljajo se mehanizmi preverjanja celovitosti, ki omogočajo zaznavanje in poročanje o nepooblaščenih spremembah.

Razpoložljivost (R):

- Vodstvo mora z načrti poslovanja redno zagotavljati zadostne vire za IKT infrastrukturo, redundantne sisteme in varnostne kopije.
- Omrežja, naprave in sistemi ne smejo biti podvrženi enotnim točkam odpovedi (ang. *single point of failure*).
- Kritični sistemi morajo imeti vnaprej definirane mehanizme za samodejni preklop (ang. *failover*) in morajo biti varovani pred napadi onemogočanja storitev.
- Varnostne kopije morajo biti hranjene v geografsko in fizično ločenih mestih, zagotovljeno mora biti redno testiranje obnove podatkov.
- Zaposleni morajo poznati postopke za delo v primeru nedosegljivosti sistemov.

Avtentičnost (A):

- Informacijski sistem mora omogočiti, da so identitete uporabnikov, naprav in sistemov preverljive in da je izvor informacij zanesljiv.
- Uporabljajo se močne metode avtentikacije, vključno z večfaktorsko avtentikacijo (MFA) in uporabo modernih avtentikatorjev, ki se upravljajo v življenjskem ciklu od izdaje do razveljavitve oziroma preklica.
- Beležiti je treba vse avtentikacijske poskuse, zagotavljati je treba reden pregled in analizo dnevnikov avtentikacije.
- Digitalni podpisi, certifikati in sistemi za preverjanje pristnosti morajo biti redno vzdrževani in posodobljeni, da zagotavljajo, da so podatki in identitete verodostojni in niso bile zlorabljene.

Odgovornost:

- Vsak uporabnik (zaposleni, pogodbeni izvajalec) je odgovoren za ravnanje s podatki, do katerih ima dostop in za sredstva, ki jih uporablja.
- Vloge in odgovornosti morajo biti jasno dokumentirane, dodeljene in redno posodabljane.
- Uporaba sistemov se beleži (Ang. *audit logs*), spremlja in analizira, da se lahko prepozna zloraba ali odstopanja.

Skladnost:

- Organizacija, njeni zaposleni in drugi uporabniki informacijskih sistemov organizacije morajo spoštovati veljavne zakone, predpise, pogodbe in notranje politike, ki urejajo informacijsko varnost.
- Vodstvo skrbi za spremljanje skladnosti, izvajanje revizij in odpravo morebitnih neskladij.
- Neupoštevanje teh načel lahko predstavlja disciplinsko odgovornost v skladu z notranjimi akti in delovnopravnimi predpisi.

Nenehno izboljševanje:

- Vodstvo redno pregleduje, ocenjuje in na podlagi rezultatov notranjih revizij, analiz incidentov in sprememb v tveganjih izboljšuje sistem upravljanja informacijske varnosti (ang. *ISMS*).
- Vodstvo, srednji management in neposredni vodje zaposlene spodbujajo, da aktivno poročajo o napakah, ranljivostih in da predlagajo izboljšave.

1.4 Zavezanost vodstva

Vodstvo aktivno podpira sistem upravljanja varovanja informacij (SUVI, ang. *ISMS*) in sistem upravljanja neprekinjenega poslovanja (SUNP, ang. *BCMS*) ter zagotavlja, da je informacijska varnost vključena v vse poslovne procese in odločitve organizacije. Še posebej:

- zagotavlja ustrezne kadrovske, finančne in tehnične vire za izvajanje in izboljševanje sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja;
- upravlja tveganja in odobri ukrepe za obvladovanje tveganj;
- vodi z zgledom in spodbuja kulturo varnosti med zaposlenimi;

- imenuje odgovorno osebo za informacijsko varnost (CISO)6, ki mora imeti ustrezna znanja, kompetence in vpliv na vodstvo, ter izvaja dolžno nadzorstvo nad njim;
- odobri izvajanje varnostnih politik in ukrepov;
- redno pregleduje učinkovitost SUVI in SUNP, obravnava rezultate notranjih in zunanjih revizij ter sprejema odločitve o izboljšavah in
- skrbi za lastno usposabljanje ter redno usposabljanje skrbnikov IKT sistemov in vseh zaposlenih na področju informacijske in kibernetske varnosti.

Vodstvo potrdi krovno in področne politike ter nosi končno odgovornost za njeno izvajanje.

1.5 Upravljanje tveganj

Upravljanje tveganj je sestavni del sistema upravljanja varovanja informacij in sistema upravljanja neprekinjenega poslovanja. Vodstvo redno izvaja postopke upravljanja tveganj za informacijsko in kibernetsko varnost, ki vključujejo identifikacijo, ocenjevanje, obravnavo in spremljanje tveganj:

- pregleda in po potrebi posodobi oceno najmanj enkrat letno ter vedno, kadar pride do pomembnih sprememb v procesih, tehnologiji ali po pomembnem varnostnem incidentu;
- odobri metodologijo za izvedbo analize obvladovanja tveganj, ki mora biti primerljiva, verodostojna in ponovljiva v skladu s pravili stroke ter vključuje popis sredstev, identifikacijo groženj in ranljivosti, oceno verjetnosti in vpliva ter ovrednotenje ravni tveganja;
- določi kriterije sprejemljivosti in sprejemljivo raven tveganja, sprejme ustrezne varnostne ukrepe za zmanjšanje ali prenos tveganja ali njegovem izogibanju, ter redno spremlja učinkovitost sprejetih ukrepov in
- dokumentira rezultate analize v registru tveganj, ki vsebuje najmanj opis tveganja, prizadeta sredstva, grožnje, ranljivosti, verjetnost, vpliv, raven tveganja in izbrane ukrepe obvladovanja.

Pri procesu upravljanja s tveganji je potrebno upoštevali tudi zunanje obveščevalne podatke kot je Ocena kibernetskih tveganj, ki jo pripravlja pristojni nacionalni organ za informacijsko in kibernetsko varnost (URSIV), ENISA objave, CSIRT in URSIV obvestila in druge empirične notranje vire, ki so na voljo v orodjih za nadzor in upravljanje informacijske in kibernetske varnosti (SIEM/MDR statistike, poročila revizij, varnostnih in drugih pregledov).

1.6 Ozaveščanje na področju informacijske in kibernetske varnosti

Vsi zaposleni in pogodbeni izvajalci organizacije, ki dostopajo do informacijskih sistemov ali podatkov organizacije, morajo vsaj enkrat letno opraviti obvezno usposabljanje s področja informacijske in kibernetske varnosti. Usposabljanje se izvede tudi ob nastopu dela, ob spremembi delovnega mesta ali uvedbi novih sistemov ter ob zaznanih spremembah v tveganjih.

Vsebina usposabljanja vključuje poznavanje osnov informacijske in kibernetske varnosti, prepoznavanje »*phishing*« napadov in drugih oblik socialnega inženiringa, varno uporabo naprav in gesel, zaščito občutljivih informacij ter postopke prijave incidentov. Usposabljanje lahko zajema tudi druge vsebine[7], ki jih priporoča pristojni nacionalni organ (URSIV), posodabljati pa se morajo tudi glede na spremembe groženj in tehnološki razvoj.

[6] CISO ni obvezna vloga po ZInfV-1; če je imenovan, lahko vodstvo nanj pod določenimi pogoji prenese nekatere naloge.
[7] https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Navodila/Priporocene-vsebine-za-osnovno-usposabljanje-s-podrocja-informacijske-in-kibernetske-varnosti.pdf

Skrbniki IKT sistemov organizacije se redno usposabljajo, da pridobijo in ohranijo raven znanj in spretnosti ter so usposobljeni za prepoznavanje in ocenjevanje tveganj ter za oceno praks obvladovanja tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja organizacija.

Vodstvo mora vsaj enkrat na štiri leta opraviti posebno usposabljanje o obvladovanju tveganj informacijske in kibernetske varnosti, kot to določa veljavna zakonodaja.

Izvedba usposabljanja mora biti dokumentirana na način, ki zagotavlja preverljivost, sledljivost in skladnost s predpisi s področja varstva osebnih podatkov in predpisov s področja dela in socialne varnosti.

Vodstvo skrbnikom IKT sistemov, vodji informacijske varnosti in drugih zaposlenim v okviru svojih zmožnosti organizira ali omogoči sodelovanje na različnih vajah s področja informacijske in kibernetske varnosti.

1.7 Upravljanje incidentov

Cilj upravljanja incidentov je zagotoviti pravočasen, točen in učinkovit odziv na incidente, zmanjšati njihov vpliv na poslovanje organizacije in drugih deležnikov ter preprečiti ponovitev podobnih dogodkov.

Organizacija ima sprejet Načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT, ki je usklajen z Nacionalnim načrtom odzivanja na kibernetske incidente[8]. Načrt vsebuje postopkovnik za zaposlene ob zaznavi suma incidenta ali podobnega varnostnega dogodka, opis sistema za zaznavo in odziv na incidente, lestvico za ocenjevanje resnosti incidenta, opis vlog in odgovornosti za odzivanje na incidente ter osnovna navodila, kaj naj stori uporabnik (npr. morebitna izolacija naprave iz omrežja).

Vsak zaposleni in drug uporabnik informacijskega sistema organizacije mora takoj prijaviti vsak sum na informacijski varnostni dogodek ali incident, tudi če ni prepričan, da gre za dejanski incident. Vse incidente je treba dokumentirati, analizirati in po potrebi sprožiti korektivne ukrepe. Med dogodke spadajo zlasti, vendar ne izključno:

- vsako neobičajno delovanje naprav (npr. nenadni ponovni zagoni, nenavadna opozorila, samodejno odpiranje programov, počasno delovanje informacijskih sistemov);
- izguba ali kraja naprave, ki vsebuje poslovne informacije (npr. prenosnik, mobilni telefon, USB ključ);
- prejem sumljive elektronske pošte (»*phishing*«, priloge neznanega ali sumljivega izvora, ipd.);
- vklop različnih alarmov;
- zaznava neavtoriziranega dostopa ali poskusa dostopa do informacijskih sistemov oziroma sredstev;
- zaznava vidno nepooblaščene fizične prisotnosti v prostorih organizacije, ki so namenjeni samo zaposlenim ali druge podobne kršitve hišnega reda organizacije;
- prejetje različnih zahtev za posodobitev ali zamenjavo občutljivih podatkov gesla, ki odstopa od ustaljenih načinov ali

[8] https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf

- potrjevanje e-pošte, zamenjava transakcijskega računa, prejem informacije o pošiljkah, ki niso bile naročene.

Incidenti se prijavljajo na elektronski naslov [E-NASLOV ORGANIZACIJE ZA PRIJAVO DOGODKOV]. V primeru, da elektronska pošta ne deluje, uporabnik uporabi druge rezervne komunikacijske kanale:

- Klic na telefon 1: [XXX XXX XXX]
- Klic na telefon 2: [XXX XXX XXX]

Zaposleni v organizaciji o zaznavi incidenta ali sumljivega dogodka takoj obvestijo tudi svojega neposredno nadrejenega in vodjo informacijske varnosti (CISO), ki zagotovi, da so vsi incidenti obravnavani v skladu z Načrtom odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT[9].

Po vsakem pomembnem incidentu se izvede analiza vzrokov, pripravi poročilo s priporočili za izboljšave in posodobi postopek glede na izkušnje in spremembe tveganj. Rezultati analiz in sprejeti ukrepi se dokumentirajo in vključijo v proces stalnega izboljševanja sistema upravljanja informacijske varnosti.

1.8 Pregled in skladnost

Neodvisna zunanja revizija skladnosti s predpisi s področja informacijske varnosti ali notranja revizija skladnosti s predpisi s področja informacijske varnosti se izvaja najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Zunanjo revizijo izvede aktivni preizkušeni revizor informacijskih sistemov, notranjo pa izvedejo notranji revizorji s sodelovanjem veščaka za informacijsko tehnologijo[10].

Samoocena skladnosti s predpisi s področja informacijske varnosti ali notranja revizija skladnosti s predpisi s področja informacijske varnosti se izvaja najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Samooceno skladnosti izvede od vodstva pooblaščena oseba z ustreznimi kompetencami na način, da dokumentirano preveri oziroma oceni skladnost organizacije s svojo interno varnostno dokumentacijo in preveri izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost. Notranjo revizijo izvedejo notranji revizorji s sodelovanjem veščaka za informacijsko tehnologijo.[11]

Pri izvedbi notranje revizije je treba zagotoviti objektivnost in nepristranskost notranjih revizorjev, ti pa ne smejo presojati svojega oddelka, lastnega dela ali svojih odločitev. Rezultati notranjih in zunanjih revizij, samoocen, varnostnih testov ter pregleda vodstva se dokumentirajo in hranijo skladno s postopki nadzora dokumentacije in dokazov sistema upravljanja varovanja informacij (SUVI, ang. ISMS) ter sistema upravljanja neprekinjenega poslovanja (SUNP, ang. *BCMS*).

Ne glede na to ali je organizacija bistven ali pomemben subjekt, mora vzdrževati celovito dokumentacijo sistema upravljanja varovanja informacij (ang. *ISMS*) ter sistema upravljanja neprekinjenega poslovanja, ki vključuje najmanj naslednje dokumente:

- krovno politiko s področnimi politikami o varnosti omrežnih in informacijskih sistemov;

[9] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan.
[10] Velja za bistvene subjekte (ne za pomembne subjekte).
[11] Velja za pomembne subjekte (ne za bistvene subjekte).

- natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih organizacija uporablja za svoje delovanje ali opravljanje storitev z določitvijo njihovih upravljavcev,
- analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo,
- politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti,
- načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih organizacija potrebuje za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja,
- načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente ter opisom vlog in odgovornosti za odzivanje na incidente,
- načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost, ki upošteva tveganja in področne posebnosti organizacije in
- politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

Vodstvo najmanj enkrat letno izvede formalni pregled sistema upravljanja varovanja informacij in sistema neprekinjenega poslovanja na podlagi rezultatov revizij, samoocen in kazalnikov učinkovitosti, ter potrdi potrebne izboljšave. Dokumentacija se posodablja tudi ob vsaki pomembni spremembi informacijskega sistema ali v rednih časovnih presledkih, na zahtevo vodstva ali nadzornega organa, najmanj pa enkrat letno[12].

Vodstvo zagotavlja tudi izvedbo varnostnega testiranja, s katerim preveri ali se ukrepi za obvladovanje tveganj za kibernetsko varnost izvajajo in ali pravilno delujejo. Varnostni testi se lahko izvajajo delno (na posameznih delih omrežja ali specifičnih informacijskih sistemih) ali kot celota.

Vključujejo lahko avtomatizirane ali ročne teste, vdorne teste za ugotavljanje, pregledovanje in izkoriščanje ranljivosti, varnostne teste za aplikacije ter konfiguracijske teste. Izvajajo se lahko ob vzpostavitvi, po nadgradnji ali spremembah infrastrukture ali aplikacij, za katere menijo, da so pomembne, ali po vzdrževanju.

Ugotovitve varnostnih testov se upoštevajo pri spremembi in dopolnitvi politik in postopkov ocenjevanja učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost ter za nenehno izboljševanje sistema upravljanja varovanja informacij in sistema neprekinjenega poslovanja.

Varnostna dokumentacija mora biti dostopna odgovornim osebam, jasno označena in nadzorovana glede sprememb.

[12] Bistveni ali pomembni subjekti so najmanj enkrat letno oziroma v rednih časovnih obdobjih, ki jih opredelijo v politiki in postopkih za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost in ob zaznanih ranljivostih, dolžni preverjati izpolnjevanje varnostnih ukrepov.

2. Področne politike informacijske varnosti

Področne politike predstavljajo izvedbeni okvir sistema upravljanja varovanja informacij in sistema neprekinjenega poslovanja. Določajo načela, pravila in odgovornosti za varno in skladno izvajanje poslovnih procesov, storitev in tehničnih rešitev.

Vse politike in ukrepi morajo biti usklajeni z veljavno zakonodajo, internimi predpisi ter tehničnimi, organizacijskimi in metodološkimi zahtevami s področja informacijske in kibernetske varnosti.

Vsaka politika določa kaj in zakaj se izvaja, postopki pa opredeljujejo kako se posamezni ukrepi izvajajo v praksi. Za vzdrževanje in pregled področnih politik je odgovorna vodja informacijske varnosti[13], njihove spremembe pa potrjuje vodstvo.

Vse kritične funkcije in sistemi morajo imeti identificirane odvisnosti, podatkovne tokove, vire, ter definirane cilje razpoložljivosti in obnovitve (ang. *RTO/RPO*).

Vsaka sprememba sistemske arhitekture, konfiguracij ali poslovnih procesov mora vključevati oceno vpliva na varnost, ki jo pregleda in odobri vodja informacijske varnosti[14].

Ključni dobavitelji in podizvajalci, ki imajo dostop do informacij, omrežij ali informacijskih sistemov, s katerimi organizacija izvaja svoje ključne storitve, morajo imeti imenovano kontaktno osebo, izvajati ustrezne varnostne ukrepe ter redno dokazovati skladnost s pogodbenimi in zakonskimi zahtevami.

Organizacija mora imeti vzpostavljene postopke za tehnično in organizacijsko preverjanje izvajalcev storitev, vključno z revizijami in pregledom dokazil o skladnosti.

Varnostna oprema, nadzorni sistemi, orodja za spremljanje in mehanizmi za zaznavanje anomalij morajo biti del enotnega okvira odzivanja na incidente, ki omogoča učinkovito obvladovanje incidentov v veh okoljih, poročanje o njih pa mora biti skladno z notranjimi postopki in zakonskimi zahtevami.

Zasnova varnostnih rešitev mora upoštevati ugotovljena tveganja, načelo odpornosti že pri zasnovi (ang. *resilience-by-design*) in načelo vseh nevarnosti (ang. *all-hazards approach*). To vključuje varno okolje, redundanco, postopke za samodejno preklapljanje delovanja (ang. *failover*), varne točke obnovitve in neodvisne komunikacijske poti.

Vse politike se redno pregledujejo najmanj enkrat letno ali po večjih spremembah v okolju, tehnologiji ali zakonodaji, da se zagotovi njihova ažurnost in učinkovitost.

Vodja informacijske varnosti[15] najmanj enkrat letno, ali po večjih spremembah v okolju, tehnologiji ali zakonodaji, pregleda področne politike in zagotavlja njihovo ažurnost ter učinkovitost, vodstvo pa jih potrdi.

2.1 Politika ozaveščanja in usposabljanja

Organizacija vzpostavlja stalni program ozaveščanja in usposabljanja, s katerim zagotavlja, da vsi zaposleni, vodstvo in zunanji sodelavci razumejo tveganja za informacijsko in kibernetsko varnost ter poznajo svoje vloge in odgovornosti pri njihovem obvladovanju.

[13] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan in kompetenten (če ni imenovan ali če ni kompetenten, je neposredna odgovornost na vodstvu).
[14] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan in kompetenten (če ni imenovan ali če ni kompetenten, je neposredna odgovornost na vodstvu).
[15] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan in kompetenten (če ni imenovan ali če ni kompetenten, je neposredna odgovornost na vodstvu).

a) Usposabljanje vodstva

Vodstvo se mora najmanj vsakih štiri (4) let udeležiti izobraževanja ali usposabljanja na področju obvladovanja tveganj informacijske in kibernetske varnosti, ki ga organizira Urad Vlade RS za informacijsko varnost ali drug strokovno priznan izvajalec.

b) Usposabljanje zaposlenih

Vsi zaposleni se najmanj enkrat letno udeležijo internega usposabljanja, ki ga organizira organizacija ali zunanji ponudnik, z namenom krepitve ozaveščenosti in prepoznavanja tveganj za informacijsko in kibernetsko varnost.

Usposabljanja morajo v čim večji meri vključevati tudi praktične primere ali primere dejanskih groženj (npr. »*phishing*« simulacije, primeri incidentov, ravnanje z informacijami).

c) Stalno strokovno usposabljanje IKT osebja

Organizacija mora omogočati, da skrbniki informacijskih sistemov, sistemski in omrežni administratorji ter druga tehnična osebja:

- redno nadgrajujejo svoje znanje na strokovnih usposabljanjih, konferencah ali strokovnih delavnicah;
- pridobivajo in vzdržujejo priznane certifikate s področja informacijske varnosti (npr. CompTIA Security+, CEH, CISSP, ISO/IEC 27001 Lead Implementer, GIAC ipd.) in
- izvajajo praktične vaje in simulacije incidentov (ang. *hands-on training*) za preverjanje odzivnosti in znanja.

Organizacija mora usposabljanja načrtovati glede na tveganja, potrebe in finančne zmožnosti, pri čemer pomanjkanje finančnih sredstev ne sme biti razlog, da se strokovna usposabljanja sploh ne izvajajo.

d) Evidentiranje in spremljanje

Izvedena usposabljanja se dokumentirajo (prisotnost, vsebina, izvajalec, datum) skladno z delovnopravnimi predpisi in predpisi s področja varstva osebnih podatkov. Vodja informacijske varnosti[16] spremlja uspešnost usposabljanj in najmanj enkrat letno poroča vodstvu o doseženi ravni ozaveščenosti in potrebnih izboljšavah.

e) Nenehno izboljševanje

Program ozaveščanja in usposabljanja se redno posodablja glede na ugotovljene potrebe, spremembe tehnologije, rezultate notranjih presoj, varnostnih incidentov in priporočila varnostnih organov (npr. pristojne CSIRT skupine).

2.2 Politika varnosti dobavne verige

Politika varnosti dobavne verige določa odgovornosti in postopke za obvladovanje tveganj, povezanih z dobavitelji in pogodbenimi izvajalci, katerih izdelki ali storitve lahko vplivajo na informacijsko in kibernetsko varnost organizacije ali na varno in neprekinjeno izvajanje storitev, ki jih organizacija zagotavlja.

[16] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan. Če ni, je spremljanje neposredna odgovornost vodstva.

a) Opredelitev in odgovornost

Organizacija vodi ažuren seznam dobaviteljev in pogodbenih izvajalcev, ki so ključni za zagotavljanje informacijske in kibernetske varnosti organizacije ali za izvajanje storitev organizacije.
Vodja informacijske varnosti[17] sodeluje pri oceni tveganj v zvezi z dobavitelji ali pogodbenimi izvajalci, pogodbenih zahtevah glede informacijske in kibernetske varnosti ter nadzoru skladnosti dobaviteljev ali pogodbenih izvajalcev.
Vodstvo zagotavlja, da so (pred podpisom pogodbe) varnostne zahteve dobavne verige vključene v procese nabave, upravljanje pogodb in obvladovanja tveganj.

b) Izbor in ocena dobaviteljev (ang. due diligence)

Pred sklenitvijo pogodbe mora biti za vsakega dobavitelja ali pogodbenega izvajalca izvedena ocena tveganja, ki vključuje:
- pregled varnostne zrelosti (npr. certifikati ISO 27001, TISAX, SOC 2), zgodovino incidentov in finančno stabilnost;
- preverjanje ukrepov in postopkov za zagotavljanje neprekinjenega poslovanja in obnove po katastrofi;
- preverjanje varnostnih praks (npr. politike dostope, obvladovanja ranljivosti, zaščita naprav, incident managementa) in
- identifikacijo ranljivosti in varnostnih tveganj, specifičnih za dobavitelja ali pogodbenega izvajalca, ter njegovo odzivnost na grožnje.

Rezultati ocene se dokumentirajo in hranijo kot del registra tveganj dobavne verige.

c) Pogodbeni okvir

Pogodbe z dobavitelji ali izvajalci morajo vključevati obvezne varnostne klavzule, med drugim:
- dolžnost varovanja zaupnosti podatkov;
- takojšnje obveščanje o ranljivostih ali incidentih;
- zagotavljanje varnosti izdelkov in storitev skozi celoten življenjski cikel;
- določitev RPO[18]/RTO[19] in načrt neprekinjenosti storitev, ki so ključne za izvajanje pogodbe;
- pravico naročnika do varnostnih presoj ali revizij dobavitelja oziroma izvajalca;
- zahteve za SBOM[20], ang. *secure software development lifecycle* (SDLC) in ang. *code signing*;
- določitev postopka za hrambo, predajo in uničenje podatkov po prenehanju pogodbe in
- razmejitev odgovornosti ter mehanizme za sankcije ob neskladnosti.

Pogodbeni pogoji morajo veljati tudi za morebitne podizvajalce dobaviteljev ali izvajalcev. Pogodbe lahko (glede na tveganja) vsebujejo tudi klavzulo o prepovedi ali omejitvi prenosa izvajanja pogodbe na podizvajalca.

[17] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan. Če ni, so te naloge neposredna odgovornost vodstva.
[18] RPO – Recover Point Objective (Ciljna točka obnovitve - Največja dopustna izguba podatkov, izražena kot čas med zadnjo varnostno kopijo (ali replikacijo) in trenutkom motnje.
[19] RTO – Recovery Time Objective (Ciljni čas obnovitve - Najdaljši dopusten čas izpada procesa, sistema ali storitve po motnji, znotraj katerega je treba ponovno vzpostaviti delovanje, da posledice ostanejo sprejemljive.
[20] SBOM - Software Bill of Materials — seznam programske opreme ali seznam sestavin programske opreme.

d) Sodelovanje in nadzor

Organizacija mora imeti vzpostavljene postopke za stalno spremljanje in obravnavo tveganj dobavne verige, vključno s periodičnim ocenjevanjem varnosti ključnih dobaviteljev in pogodbenih izvajalcev.

Ključni dobavitelji in pogodbeni izvajalci morajo:
- zagotavljati postopke za razkritje in odpravljanje ranljivosti (ang. *vulnerability disclosure policy*),
- redno posodabljati sisteme in odpravljati znane ranljivosti in
- dokazovati uporabo varnostnih ukrepov (SDLC, varno programiranje, nadzor dostopov, varnost v oblaku).

Organizacija ima pravico zahtevati dokazila o skladnosti (certifikate, poročila presoj, rezultate testov).

Skrbnik pogodbe spremlja izvajanje varnostnih določil in poroča vodji informacijske varnosti[21] ter vodstvu.

e) Prenehanje sodelovanja

Ob prenehanju sodelovanja mora dobavitelj ali pogodbeni izvajalec:
- varno odstraniti ali vrniti vse podatke in kopije;
- preklicati vse dostopne pravice in poverilnice in
- predložiti potrdilo o uničenju podatkov in zaključnem pregledu skladnosti (ang. *exit compliance review*).

[21] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan.

f) Upoštevanje zunanjih ocen tveganja

Organizacija mora pri svoji oceni in ukrepih upoštevati tudi rezultate usklajenih ocen tveganja za kritične dobavne verige, ki jih pripravljajo Skupina za sodelovanje[22], ENISA ali pristojni nacionalni organ.

g) Izhodna strategija (Ang. exit strategy)

Organizacija mora sprejeti ukrepe za primer nenadne in nepredvidene odpovedi pogodbe na strani ključnih dobaviteljev ali ponudnikov storitev. Za vsako ključno storitev mora biti predhodno na trgu identificiran alternativni ponudnik.

Pri najemanju oblačnih storitev mora organizacija sprejeti in izvajati ukrepe, ki omogočajo nemoteno zamenjavo ponudnika (npr. ustrezen format podatkov, kopije produkcijskih konfiguracijskih datotek ključnih naprav).

2.3 Politika nadzora dostopa

Politika nadzora dostopa ureja dodeljevanje, uporabo in nadzor uporabniških pravic za dostop do informacijskih sistemov, aplikacij in storitev organizacije, z namenom zagotavljanja načela najmanjših privilegijev, sledljivosti in varne avtentikacije uporabnikov.

a) Dodeljevanje in vodenje dostopov

- dostopi se dodeljujejo na podlagi vnaprej določenih vlog in odgovornosti;
- vsak dostop mora biti odobren s strani nadrejenega in evidentiran;
- uporabniški računi morajo biti individualni in neprenosljivi;
- pravice dostopa se revidirajo najmanj vsakih šest mesecev ali po vsaki kadrovski spremembi in
- računi, ki se ne uporabljajo več kot 90 dni, se samodejno deaktivirajo.

b) Avtentikacija in gesla navadnih uporabnikov

- gesla morajo biti dolga najmanj 12 znakov; dovoljena je uporaba vseh znakov, vključno s presledki;
- gesel ni treba menjati periodično, ampak le ob sumu ali potrjeni kompromitaciji;
- gesla se morajo preverjati glede na sezname kompromitiranih gesel (ang. *blacklist*) in zavrniti, če so prepoznana kot šibka ali javno objavljena;
- hramba gesel mora zagotavljati kriptografsko zaščito s “salt + hash” (npr. *bcrypt, scrypt* ali Argon2),
- prepovedano je obrezovanje gesel (ang. *password truncation*),
- uporaba organizacijsko odobrenih upravljavcev gesel (ang. *password manager*) je dovoljena in priporočena in
- hramba gesel v brskalnikih je prepovedana.

[22] Skupina za sodelovanje je organ, ustanovljen na podlagi 14. člena Direktive (EU) 2022/2555 (t. i. Direktiva NIS 2), sestavljen iz predstavnikov držav članic Evropske unije, Evropske komisije in Agencije Evropske unije za kibernetsko varnost (ENISA). Njene naloge vključujejo izmenjavo dobrih praks, pripravo smernic za pristojne nacionalne organe, usklajeno ocenjevanje kibernetskih tveganj (vključno s tveganji v dobavnih verigah) ter prispevek k vzajemnim pregledom in čezmejnemu sodelovanju na področju kibernetske varnosti.

c) Večfaktorska avtentikacija (ang. MFA)

- večfaktorska avtentifikacija je obvezna za vse oddaljene dostope (VPN, VDI, e-pošta v oblaku ipd.), za vse administrativne in sistemske račune, ter za druge sisteme, kjer to zahteva ocena tveganja in
- večfaktorska avtentifikacija mora uporabljati vsaj dve neodvisni metodi preverjanja (npr. geslo + biometrija ali geslo + varnostni ključ).

d) Zaklepanje računov in nadzor prijav

- računi se zaklenejo po 5 neuspelih poskusih prijave;
- trajanje zaklepa: najmanj 15 minut ali do ročnega odklepa s strani administratorja in
- aktivnosti prijav se beležijo in spremljajo za zaznavanje sumljivih vzorcev prijav.

e) Administrativni in privilegirani računi

- Vsak administrator mora imeti ločene račune za:
  - vsakodnevno delo (navaden uporabniški račun);
  - administrativna opravila (admin račun) in
  - v primeru večje organizacije, poseben “super-admin” račun z dodatnimi omejitvami.
- Administrativni računi:
  - se uporabljajo izključno za administrativna opravila;
  - morajo imeti geslo z najmanj 16 znaki in obvezno MFA;
  - vse aktivnosti morajo biti beležene in redno pregledovane in
  - vsaka uporaba mora biti utemeljena in dokumentirana.
- Gesla “super-admin” računov se hranijo v fizični obliki v zapečatenem sefu pod nadzorom vodje informacijske varnosti[23]; dostop je dovoljen samo po postopku dvostopenjske odobritve.
- Za potrebe obnove sistemov ob izrednih dogodkih se kopija teh gesel hrani ločeno, z dostopom samo pooblaščenih oseb.

f) Prijava, odjava in spremljanje

- uporabniki morajo zakleniti delovno postajo, kadar je brez nadzora;
- seje se samodejno prekinejo po največ 15 minutah nedejavnosti in
- vsi dogodki prijav, sprememb pravic in zaklepov se dnevniško beležijo in varno hranijo.

g) Načelo najmanjšega privilegija in revizija

- vodstvo in lastniki sistemov morajo zagotoviti, da ima vsak uporabnik dostop le do tistih virov, ki jih nujno potrebuje in
- pregled dostopov se izvaja najmanj vsakih šest (6) mesecev ali ob večjih spremembah organizacijske strukture.

h) Kontinuiran nadzor in izboljšave

- vodja informacijske varnosti[24] spremlja učinkovitost ukrepov nadzora dostopa in predlaga izboljšave na podlagi analiz incidentov, notranjih presoj in sprememb tehnologij.

[23] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, mora nadzor izvesti vodstvo neposredno.
[24] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, mora te naloge izvajati vodstvo.

2.4 Politika ravnanja s sredstvi

Politika ravnanja s sredstvi določa način identifikacije, popisa, klasifikacije, vrednotenja, uporabe in odstranjevanja informacijskih in drugih sredstev organizacije. Namen politike je zagotoviti celovit nadzor nad vsemi sredstvi, ki so potrebna za varno in neprekinjeno izvajanje storitev, ki jih organizacija zagotavlja.

a) Popis sredstev

- Organizacija mora vzpostaviti in vzdrževati celovit popis vseh sredstev, ki obsega najmanj:
  - strojno in komunikacijsko opremo (strežniki, delovne postaje, omrežna oprema, IoT[25] naprave ipd.);
  - programsko opremo (operacijski sistemi, aplikacije, licence, baze podatkov);
  - informacijske vsebine in podatke (v digitalni in fizični obliki);
  - pogodbe / SLA[26] za storitve in zunanje ponudnike (vključno z oblačnimi storitvami);
  - prostore, infrastrukturo in fizično okolje in
  - osebje, ki ima dodeljene odgovornosti in dostop do informacijskih sistemov.

- Popis se vodi v registru sredstev, ki mora vsebovati vsaj naslednje podatke:
  - enolično oznako sredstva;
  - ime sredstva in vrsto;
  - lastnika oziroma skrbnika sredstva;
  - lokacijo sredstva;
  - opis funkcije sredstva;
  - klasifikacijo po zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (Z, C, R, A ali ang. C, I, A, Au);
  - datum - konec življenjske dobe sredstva (konec podpore, pogodbe, licence, nadgradenj in podobno kar je relevanten podatek za sredstvo)
  - odvisnosti od drugih sredstev in povezavo z izvajanjem storitev;
  - povezavo sredstva s poslovnim procesom ali storitvijo, ki ga uporablja, ter povezavo s cilji RTO in RPO, določenimi v analizi vpliva na poslovanje in
  - datum uvedbe, spremembe ali izločitve sredstva.

b) Lastništvo in odgovornost

- Vsako sredstvo mora imeti določenega lastnika ali skrbnika, ki je odgovoren za:
  - redno posodabljanje podatkov o sredstvu;
  - oceno vrednosti in tveganj, povezanih s sredstvom;
  - določitev potrebnih varnostnih ukrepov in
  - odobritev sprememb, premikov ali izločitve sredstva.
- Vse spremembe lastništva ali premiki sredstev morajo biti dokumentirani in odobreni.

c) Klasifikacija in vrednotenje

- Sredstva se razvrstijo po stopnji zaupnosti, celovitosti, razpoložljivosti in avtentičnosti.
- Za vsako sredstvo se določi njegov vpliv na izvajanje storitev in poslovnih procesov ter povezava s cilji RTO in RPO, določenimi v analizi vpliva na poslovanj.

[25] IoT – Internet of Things - kratica označuje omrežje fizičnih naprav, vozil, senzorjev in drugih predmetov, ki so povezani prek interneta in med seboj izmenjujejo podatke.
[26] SLA - Service Level Agreement – dogovor o ravni storitev.

- Kritična sredstva so tista, katerih nedelovanje bi ogrozilo izvajanje storitev iz prilog 1, 2 ali 3 ZInfV-1.

d) Spremljanje in revizija popisa

- Popis sredstev se redno posodablja; vsaj enkrat letno se izvede revizija registra sredstev.
- Organizacija mora zagotoviti tehnična orodja za zaznavanje novih ali nepooblaščenih sredstev v omrežju.
- Lastniki sredstev morajo potrditi spremembe.

e) Izločitev in odstranjevanje sredstev

- Ob izločitvi sredstva je treba zagotoviti popolno brisanje podatkov (npr. s postopki, skladnimi z metodami DoD 5220.22-M[27] ali NIST SP 800-88).
- Izločitev mora biti dokumentirana, vključno z datumom in podpisom odgovorne osebe.

f) Povezava z drugimi procesi

- Register sredstev predstavlja osnovo za analizo tveganj, načrte neprekinjenega poslovanja, oceno vpliva na poslovanje in načrt obnovitve po nesreči.
- Vodja informacijske varnosti[28] skrbi, da se popis sredstev uporablja kot izhodišče pri vseh procesih upravljanja tveganj in izvajanju varnostnih presoj.

2.5 Politika varnosti človeških virov

Politika varnosti človeških virov določa obveznosti, odgovornosti in ukrepe, s katerimi organizacija zagotavlja, da imajo zaposleni in pogodbeni sodelavci ustrezno stopnjo zaupanja, zavedanja in odgovornosti pri delu z informacijami in informacijskimi sistemi organizacije. S tem organizacija zmanjšuje tveganja, povezana s človeškim dejavnikom, in zagotavlja, da vsi deležniki razumejo ter spoštujejo zahteve informacijske in kibernetske varnosti.

a) Postopki organizacije pred zaposlitvijo

- Organizacija določi varnostne zahteve in odgovornosti za vsako delovno mesto, zlasti za tista, ki vključujejo dostop do informacijskih sistemov ali občutljivih podatkov.
- Za kandidate za delovna mesta, ki vključujejo dostop do informacijskih sistemov ali občutljivih podatkov, organizacija posebno skrbno izvede preverjanje referenc, izobrazbe, strokovnih kompetenc in usposobljenosti.
- Na podlagi ocene tveganja organizacija za kandidate za delovna mesta, na katerih bodo imeli zaposleni neposredni ali oddaljeni dostop do ključnih informacijskih sistemov organizacije, izvaja preverjanje preteklosti kandidatov ali zaposlenih v skladu z obsegom in pogojih iz 23. člena ZInfV-1.
- Preverjanje se izvaja tudi za zaposlene dobaviteljev ali pogodbenih izvajalcev, če bodo imeli dostop do ključnih informacijskih sistemov organizacije; način in izvedba preverjanja se v tem primeru določita v pogodbi z dobaviteljem ali pogodbenim izvajalcem.
- Pred začetkom zaposlitve morajo kandidati ali pogodbeni sodelavci podpisati izjavo o zaupnosti oziroma sporazum o nerazkritju.

[27] Postopek, ko se podatke na magnetnih nosilcih večkrat prepiše s kombinacijo ničel, enic in naključnih vzorcev.
[28] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, mora te naloge izvajati vodstvo.

- Pogodbe o zaposlitvi ali sodelovanju morajo vsebovati določila o informacijski varnosti, dolžnosti varovanja poslovnih skrivnosti in drugih občutljivih podatkov organizacije ter obveznosti spoštovanja internih politik organizacije.

b) Postopki organizacije med zaposlitvijo:

- Vsi zaposleni in pogodbeni sodelavci se morajo redno usposabljati o informacijski in kibernetski varnosti, najmanj enkrat letno, organizacija pa hrani dokazila o izvedbi usposabljanj skladno s predpisi o delovnih razmerjih, evidencah s področja dela in socialne varnosti in varstvu osebnih podatkov.
- Organizacija izvaja ali omogoči izvajanje ciljno usmerjenih usposabljanja glede na vlogo zaposlenega (npr. skrbniki sistemov, vodje projektov, vodstvo).
- Organizacija zagotavlja, da so vsi zaposleni in pogodbeni sodelavci seznanjeni s politikami, svojimi odgovornostmi glede varovanja informacij in postopki obveščanja o incidentih, zaposleni in pogodbeni sodelavci pa morajo te politike, odgovornosti in postopke spoštovati in izvajati.
- Vodja informacijske varnosti[29] spremlja spoštovanje in izvajanje politik informacijske varnosti, kršitve se obravnavajo skladno z notranjimi postopki in pogodbenimi določili.
- Osebe, ki so predmet preverjanja preteklosti po ZInfV-1, so dolžne nemudoma obvestiti organizacijo o vsakem dogodku ali postopku, ki bi lahko vplival na njihovo zanesljivost (npr. kazenska obsodba, izguba pooblastil, varnostni incident); ne-obveščanje se obravnava kot kršitev skladno z notranjimi postopki in pogodbenimi določili.
- Pristojna služba organizacije dostope zaposlenih in pogodbenih sodelavcev do informacijskih sistemov in podatkov redno pregleduje in prilagaja spremembam vlog ali odgovornosti.

c) Postopki organizacije ob prenehanju ali spremembi zaposlitve:

- Zaposlenemu ob prenehanju zaposlitve takoj prenehajo vse pravice dostopa do informacijskih sistemov in fizičnih lokacij organizacije.
- Neposredni vodja enote, v kateri je osebi prenehala ali je bila spremenjena zaposlitev, mora o prenehanju ali spremembi zaposlitve nemudoma obvestiti enoto, ki je pristojna za uporabniške račune in dostopne pravice.
- Za pogodbene sodelavce se način obveščanja o spremembah iz prejšnje alineje določi v pogodbi.
- Organizacijska enota, ki je pristojna za uporabniške račune in dostopne pravice mora preklicati ali prilagoditi vse uporabniške račune in dostopne pravice najpozneje v 24 urah po prenehanju ali spremembi vloge.
- Zaposleni mora vrniti vse službene naprave, nosilce podatkov in dokumentacijo najpozneje zadnji delovni dan.
- Če organizacija zaposlenemu dovoli zasebno uporabo službene naprave (npr. mobilnega telefona) tudi po prenehanju zaposlitve, mora enota, pristojna za uporabniške račune in dostopne pravice, pred izročitvijo naprave osebi s te naprave izbrisati vse službene podatke in aplikacije ali jo ponastaviti na tovarniške nastavitve.
- Po prenehanju zaposlitve se lahko izvede izstopni razgovor, pri katerem se zaposlenega opozori na obveznost varovanja zaupnih informacij tudi po prenehanju delovnega razmerja.
- Če se spremeni delovno mesto v organizaciji, organizacija izvede novo oceno dostopa glede na novo vlogo in tveganja.

[29] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, mora te naloge izvajati vodstvo.

2.6 Politika fizične in okoljske varnosti

Politika fizične in okoljske varnosti določa ukrepe za preprečevanje nepooblaščenega fizičnega dostopa, škode ali motenj v delovanju informacijskih sistemov, infrastrukture in podatkov organizacije. Namen politike je zagotoviti ustrezno zaščito ljudi, prostorov, naprav in informacijskih sredstev pred naravnimi, tehničnimi in človeškimi grožnjami.

a) Organizacija fizičnega varovanja

- Vsi prostori, kjer se nahajajo ključna informacijska sredstva, morajo biti ustrezno zaščiteni pred nepooblaščenim vstopom, poškodbami, požarom in okoljskimi vplivi.
- Če je organizirana služba varovanja z varnostno službo, se fizično in tehnično varovanje izvaja skladno z Zakonom o zasebnem varovanju (ZZasV-1) in Uredbo o obveznem organiziranju varovanja, podrobnosti o organizaciji fizičnega in tehničnega varovanja pa se opredelijo v načrtu varovanja.
- Dostop v poslovne prostore organizacije je dovoljen le po predhodni identifikaciji zaposlenih in obiskovalcev (npr. osebni dokument); če ima organizacija lastno upravno območje, se za dostop upoštevajo tudi predpisi s področja varstva tajnih podatkov.
- Vsi obiskovalci morajo biti spremljani in evidentirani, razvidna morata biti namen in lokacija obiska.

b) Zaščita ključnih prostorov

- Prostori, kjer se nahajajo ključni informacijski sistemi organizacije, morajo biti posebej zaščiteni. To so najmanj:
  - strežniške sobe in podatkovni centri;
  - prostori s ključno komunikacijsko in omrežno opremo;
  - prostori s sistemi za varnostno kopiranje in hranjenje medijev;
  - prostori z opremo za neprekinjeno napajanje (UPS, agregati) in
  - kontrolni centri ali tehnični prostori, kjer se upravlja informacijska infrastruktura.
- Dostop do ključnih prostorov je omogočen le z večfaktorsko avtentikacijo (npr. elektronska kartica in ključ, elektronski ključ in PIN koda, kartica in mobilna koda ipd.).
- Vstopi v ključne prostore se evidentirajo (vključno z uro izstopa), evidence pa se skladno z ZVOP-2 hranijo največ dve leti od konca koledarskega leta po vnosu osebnih podatkov v zbirko, nato se izbrišejo ali na drug način uničijo; evidenca sme vsebovati le nabor podatkov iz 85. člena ZVOP-2.
- Ključni prostori morajo biti varovani z alarmnim sistemom in nadzorovani z video nadzorom; uporaba in upravljanje sistemov video nadzora morata biti skladna s predpisi s področja varstva osebnih podatkov in zasebnega varovanja in se ne smejo uporabljati za drug namen, kot je določeno s temi predpisi.
- Ključna oprema mora biti fizično pritrjena ali zaklenjena (npr. stojala, omare, rack-sistemi).
- V primeru vzdrževanja ali nujnih del je dostop dovoljen le ob prisotnosti pooblaščene osebe organizacije.

c) Okoljska zaščita in napajanje

- Organizacija mora zagotoviti ustrezne okoljske pogoje (temperaturo, vlago, prezračevanje, preprečevanje poplav in prahu) v vseh prostorih, kjer se nahajajo ključni informacijski sistemi.
- Ključni prostori iz morajo biti opremljeni s senzorji, ki merijo pogoje iz prejšnje alineje.

- Vzpostavljena mora biti požarna zaščita, skladna s požarnim načrtom organizacije, vključno s sistemi za zgodnje odkrivanje in gašenje požara (npr. senzorji dima, avtomatski gasilni sistemi, ročni gasilniki, pri čemer mora biti vrsta gasilnika prilagojena možnemu razredu požara).
- Sistem za neprekinjeno napajanje (ang. *UPS*) mora zagotavljati napajanje toliko časa, kolikor je potrebno za varen preklop na rezervni vir napajanja.
- Rezervni vir napajanja (npr. agregat) mora biti ustrezno zmogljiv in založen z gorivom, da pokrije oskrbo vsaj ključnih procesov organizacije do ponovne vzpostavitve redne oskrbe z električno energijo.
- UPS sistemi in agregati se testirajo najmanj enkrat mesečno, preverja pa se tudi njihova funkcionalnost in zaloga goriva.
- Vsi posegi v okoljsko infrastrukturo (elektrika, klimatizacija, varnostne naprave, senzorji) morajo biti odobreni, dokumentirani in nadzorovani.

d) Zaščita fizičnih medijev in opreme

- Fizični mediji (varnostne kopije, prenosni nosilci, arhivski diski ipd.) morajo biti shranjeni v zaklenjenih in nadzorovanih prostorih, premiki ali iznosi teh medijev morajo biti odobreni in evidentirani.
- Infrastruktura, ki omogoča centralizirano varnostno kopiranje ali avtomatizirano upravljanje konfiguracij, mora biti fizično in logično zaščitena ter dostopna samo pooblaščenim osebam.
- Glavni komunikacijski vodi in ožičenje ključnih naprav mora biti izven ključnih prostorov zaščiteno.
- Za hrambo varnostnih kopij in ključnih medijev mora biti zagotovljena fizična ločenost lokacij (ang. *off-site storage*) skladno s politiko varnostnega kopiranja (poglavje 2.8).

e) Preverjanje in testiranje

- Učinkovitost fizičnih in okoljskih varnostnih ukrepov se redno preverja (najmanj enkrat letno) in po večjih spremembah infrastrukture;
- Rezultati preverjanj in testov se dokumentirajo, odstopanja pa se obravnavajo kot varnostni incidenti ali neskladnosti.
- Organizacijska enota, ki je pristojna za uporabniške račune in dostopne pravice, redno preverja veljavnost dostopnih pravic do varovanih prostorov in ažurira evidence.

f) Odgovornost in skladnost

- Vodja informacijske varnosti[30] skrbi za skladnost ukrepov fizične in okoljske varnosti z drugimi področnimi politikami in dokumenti (npr. politiko nadzora dostopa, politiko varnostnega kopiranja, načrtom neprekinjenega poslovanja),
- Če fizično ali tehnično varovanje izvaja varnostna služba, se v pogodbi določijo tudi obveznosti iz te politike.

2.7 Politika upravljanja z ranljivostmi in posodobitvami

Politika upravljanja z ranljivostmi in posodobitvami določa načela in postopke za pravočasno odkrivanje, ocenjevanje, odpravljanje in spremljanje tehničnih ranljivosti na informacijskih in komunikacijskih sistemih organizacije.

[30] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, mora te naloge izvajati vodstvo.

Namen politike je zmanjšati možnost izrabe ranljivosti in s tem vpliv na zaupnost, celovitost, razpoložljivost in avtentičnost informacijskih sredstev ter storitev organizacije.

a) Identifikacija ranljivosti

- Organizacija mora spremljati in prepoznavati ranljivosti na vseh informacijskih in komunikacijskih sredstvih, vključno s strežniki, delovnimi postajami, omrežno in varnostno opremo, aplikacijami, oblačnimi storitvami in mobilnimi napravami.
- Skrbniki informacijskih sistemov morajo redno spremljati varnostna obvestila proizvajalcev, objave skupin CSIRT, sezname znanih ranljivosti (npr. CISA KEV, CVE) in druge relevantne vire informacij.
- Organizacija mora uporabljati orodja za avtomatizirano zaznavanje ranljivosti (ang. *vulnerability scanning*) z ustreznimi pooblastili (ang. *credentialed scan*), skeniranje pa mora zajemati tako zasebni del omrežja, kot javno izpostavljeni del.
- Vse zaznane ranljivosti se vpišejo v enoten register ranljivosti, ki omogoča sledljivost celotnega postopka (od zaznave do zaprtja).
- Ranljivosti razvrstijo po kritičnosti pri čemer se uporabi ena od priznanih metod za opredelitev kritičnosti ranljivosti. (Primer: CVSS[31])
- Organizacija lahko dopolni oceno kritičnosti, ki jo običajno podajo orodja za avtomatizirano zaznavanje ranljivosti s poslovnim kontekstom, pri čemer se poleg ocene CVSS upošteva še poslovna kritičnost sredstva in izpostavljenost.

b) Odpravljanje ranljivosti in roki za ukrepanje

- Ranljivosti se morajo odpraviti ali ublažiti v roku, ki je sorazmeren s stopnjo tveganja in kritičnostjo sredstva:
  - kritične (internetno izpostavljene): odprava ali kompenzacijski ukrep najpozneje v 72 urah po objavi popravka ali potrditvi izrabe;
  - kritične (notranje): odprava ali ublažitev v 7 dneh;
  - visoke: odprava v 14 dneh;
  - srednje: odprava v 30 dneh in
  - nizke: odprava v 90 dneh.
- V ločenih okoljih (npr. OT okolje, ločeno od IT in interneta z IDMZ[32]) se posodobitve in popravki nameščajo preko »*jump*« strežnikov.
- V primeru sistemov, kjer popravka ni mogoče uporabiti (npr. OT sistemi z zastarelo ali nepodprto »legacy« opremo), se morajo skladno z oceno tveganja in načrtom varnostnih ukrepov izvajati ukrepi za blaženje tveganja (npr. segmentacija, izolacija v IDMZ, (ang. *whitelisting, virtual patching)*, dodatni nadzor, ipd.).
- Izjeme od rokov mora pisno odobriti vodja informacijske varnosti, odobritev mora biti dokumentirana in časovno omejena.
- Vsi nameščeni varnostni popravki in kompenzacijski ukrepi morajo biti dokumentirani, zagotovljena mora biti sledljivost v registru ranljivosti.

c) Testiranje in uvedba sprememb

- Namestitev popravkov se izvaja po postopku upravljanja sprememb (ang. *change management*), z vnaprejšnjo potrditvijo, dokumentiranjem in možnostjo povrnitve (ang. *rollback*).

[31] CVSS - Common Vulnerability Scoring System. Najbolj razširjena metoda je CVSS, ki jo vzdržuje organizacija FIRST.org (trenutno različica v3.1, kmalu v4.0).
[32] IDMZ - Identity Demilitarized Zone. Gre za posebno varnostno območje v IKT-arhitekturi, namenjeno zaščitenemu posredovanju identitetnih storitev med zunanjim omrežjem (npr. internetom) in notranjim omrežjem organizacije.

- Za kritične ranljivosti z aktivno izrabo se lahko uporabi nujni postopek (ang. *emergency change*), o čemer se po izvedbi pripravi poročilo za vodjo informacijske varnosti.
- Popravki se morajo testirati v ločenem okolju, kadar je to mogoče, pred uvedbo v produkcijo.
- Po izvedbi popravka ali spremembe se mora izvesti verifikacija delovanja in varnosti sistema.

d) Preverjanje učinkovitosti in spremljanje

- Po namestitvi popravkov se izvede ponovno preverjanje (ang. *rescan*) v roku 7 dni od namestitve.
- Če ranljivost po ponovnem pregledu ni odpravljena, se določijo dodatni ukrepi ali eskalacija lastniku sistema.
- Organizacija mora spremljati in meriti učinkovitost postopkov upravljanja z ranljivostmi z naslednjimi kazalniki:
  - delež odpravljenih ranljivosti v predpisanem roku (ang. *SLA*);
  - povprečni čas odprave (ang. *MTTR*) po stopnji resnosti;
  - število aktivnih izjem;
  - delež ranljivosti s potrjeno aktivno izrabo in
- o rezultatih se najmanj enkrat letno poroča vodstvu in vodji informacijske varnosti.

e) Upravljanje z ranljivostmi pri zunanjih izvajalcih

- Zunanji izvajalci in ponudniki storitev, ki vzdržujejo ali gostujejo informacijske sisteme organizacije, morajo spoštovati enake ali strožje zahteve glede rokov in varnostnih postopkov.
- Obveznosti glede odprave ranljivosti in posodobitev se določijo v pogodbi ali dogovoru o ravni storitev (SLA).
- Zunanji izvajalec mora redno ali na zahtevo organizacije predložiti dokazila o izvedenih posodobitvah, poročila o skeniranju ali izjavo o skladnosti.

f) Odgovornost in skladnost

- Za izvajanje postopkov upravljanja z ranljivostmi so odgovorni skrbniki posameznih sredstev ali sistemov v sodelovanju z vodjo informacijske varnosti[33].
- Vodja informacijske varnosti[34] zagotavlja skladnost z drugimi področnimi politikami in dokumenti (npr. politiko nadzora dostopa, politiko varnostnega kopiranja, načrtom neprekinjenega poslovanja in politiko razvoja programske opreme).
- Celoten postopek upravljanja z ranljivostmi mora biti dokumentiran in sledljiv ter se izvaja skladno s postopki sprememb in obvladovanja incidentov.

2.8 Politika varnostnega kopiranja

Politika varnostnega kopiranja določa zahteve in postopke za redno izdelavo, hrambo, zaščito, testiranje in obnovo varnostnih kopij podatkov, aplikacij in konfiguracij informacijskih sistemov. Namen politike je zagotoviti razpoložljivost in celovitost podatkov ter neprekinjeno delovanje organizacije v primeru izgube, poškodbe ali odtujitve podatkov.

[33] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, je odgovornost neposredno na vodstvu.
[34] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, je odgovornost neposredno na vodstvu.

a) Obseg in načela

- Organizacija mora izvajati varnostno kopiranje vseh podatkov, konfiguracijskih datotek, aplikacij in sistemskih nastavitev, ki so pomembni za izvajanje njenih storitev.
- Politika varnostnega kopiranja velja za vse IKT sisteme in okolja, vključno s strežniki, delovnimi postajami, virtualnimi okolji in oblačnimi storitvami.
- Če so del IKT sistema in okolja organizacije tudi sistemi zunanjih izvajalcev, se jih s pogodbo/SLA zaveže k enakemu obsegu in načelom, kot veljajo za organizacijo.
- Frekvenca in obseg varnostnega kopiranja morata biti usklajena s cilji RTO (ang. *Recovery Time Objective*) in RPO (ang. *Recovery Point Objective*), ki izhajata iz analize vpliva na poslovanje.

b) Izvajanje varnostnega kopiranja

- Varnostno kopiranje se izvaja samodejno po vnaprej določenem urniku.
- Za vse podatke, ki so ključni za delovanje organizacije, se varnostne kopije izvajajo dnevno.
- Manj kritični podatki se kopirajo tedensko ali po potrebi, glede na oceno tveganja in dogovorjene cilje RTO/RPO.
- Izvaja se 3-2-1 pravilo varnostnega kopiranja:
  - najmanj tri kopije podatkov (ena primarna in dve varnostni);
  - hranjene na dveh različnih medijih in
  - pri čemer je ena kopija shranjena ločeno od primarne lokacije (ang. *off-site*) ali v načinu ločenem od omrežja (ang. *off-line*).
- Vse varnostne kopije morajo biti šifrirane z močnimi algoritmi in zaščitene pred nepooblaščenim dostopom.
- Dostop do sistemov za varnostno kopiranje je dovoljen samo pooblaščenim osebam z uporabo večfaktorske avtentikacije.

c) Hranjenje in zaščita varnostnih kopij

- Varnostne kopije se hranijo v prostorih, ki so fizično ločeni od primarne infrastrukture in ustrezno zaščiteni pred požarom, vodo, prahom in nepooblaščenim dostopom.
- Kopije morajo biti zaščitene tudi pred napadi z zlonamerno programsko opremo, zato mora biti vsaj ena kopija hranjena v »offline« ali »immutable« načinu.
- Čas hrambe varnostnih kopij se določi glede na pravne, regulativne in poslovne zahteve ter klasifikacijo podatkov.
- Po izteku obdobja hrambe se varnostne kopije varno izbrišejo ali uničijo v skladu s postopkom uničenja podatkov.

d) Preverjanje in testiranje obnovljivosti

- Uspešnost varnostnega kopiranja se mora samodejno preverjati po vsakem postopku kopiranja.
- Napake ali neuspešne kopije se morajo takoj evidentirati in analizirati.
- Obnovljivost podatkov se mora testirati najmanj četrtletno in po vsaki pomembni spremembi informacijskega sistema.
- Testi obnove morajo preverjati tako celovitost podatkov kot delovanje aplikacij po obnovi.
- Rezultati testov obnove se dokumentirajo, neskladnosti pa se odpravijo v dogovorjenem roku.

e) Evidentiranje in nadzor

- Vsi postopki varnostnega kopiranja in obnavljanja morajo biti zabeleženi v dnevnikih (ang. *log*) z navedbo datuma, časa in obsega.
- Varnostne kopije in pripadajoči sistemi morajo biti vključeni v register informacijskih sredstev.
- O vsaki napaki pri varnostnem kopiranju ali neuspešni obnovi mora biti obveščen vodja informacijske varnosti[35].
- V primeru kritične napake ali izgube podatkov se sproži postopek upravljanja incidentov.

f) Odgovornost in skladnost

- Za izvajanje, preverjanje, obnovo varnostnih kopij in pregled dnevniških zapisov varnostnega kopiranja so odgovorni skrbniki sistemov v sodelovanju z vodjo informacijske varnosti.
- Vodja informacijske varnosti skrbi za skladnost politike varnostnega kopiranja z načrtom neprekinjenega poslovanja in načrtom obnovitve po nesreči.
- Vse spremembe sistemov za varnostno kopiranje morajo biti odobrene, dokumentirane in preverjene po postopku upravljanja sprememb.

2.9 Politika kriptografije

Politika kriptografije določa načela, standarde in postopke za zaščito podatkov z uporabo kriptografskih mehanizmov. Namen politike je zagotoviti zaupnost, celovitost, razpoložljivost in avtentičnost podatkov ter preprečiti nepooblaščen dostop, spremembe ali razkritja informacij.

a) Uporaba kriptografije

- Podatki v prenosu morajo biti zaščiteni z uporabo varnih protokolov (najmanj TLS 1.2, priporočeno TLS 1.3).
- Uporaba zastarelih in ranljivih protokolov (npr. SSLv2, SSLv3, TLS 1.0, TLS 1.1) je prepovedana.
- Za zaščito podatkov v mirovanju se morajo uporabljati kriptografski algoritmi, skladni s FIPS 140-3 ali enakovrednimi standardi.
- Prenosne naprave, prenosni mediji in prenosni računalniki morajo imeti šifrirane diske ali particije (npr. BitLocker, VeraCrypt, LUKS, ipd.).
- Vse baze podatkov, ki vsebujejo občutljive informacije ali osebne podatke, morajo biti šifrirane v mirovanju (ang. *data-at-rest encryption*).

b) Algoritmi in standardi

- Uporabljajo se samo sodobni in preverjeni kriptografski algoritmi, kot so AES (256-bit), RSA (2048-bit ali več), ECC (P-256 ali močnejši), SHA-2 (256-bit).
- Uporaba algoritmov MD5, SHA-1, DES ali 3DES je prepovedana.
- Pri izbiri algoritmov je treba upoštevati odpornost na kvantne napade (ang. *post-quantum cryptography – PQC*).
- Pri nabavi novih IKT rešitev ali opreme mora organizacija preveriti, ali proizvajalec zagotavlja podporo za postkvantne algoritme in hkrati združljivost z obstoječimi standardi.
- Kriptografski algoritmi in konfiguracije se morajo redno preverjati glede skladnosti s standardi in priporočili (npr. ENISA, NIST, SANS).

[35] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, se obvesti neposredno vodstvo.

c) Upravljanje ključev in certifikatov

- Vsi kriptografski ključi, digitalni certifikati in zasebni ključi morajo imeti določen življenjski cikel: generiranje, distribucijo, uporabo, rotacijo, preklic in uničenje.
- Ključi morajo biti zaščiteni z gesli in shranjeni v varnih shrambah (HSM, TPM, KeyVault),
- Upravljanje ključev mora vključevati načelo ločevanja vlog (ustvarjanje, potrjevanje, distribucija).
- Vse certifikate mora izdati zaupanja vreden overitelj (ang. *certificate authority*).
- Strežniški in sistemski certifikati morajo biti vključeni v nadzorni sistem, ki omogoča spremljanje veljavnosti in pravočasno opozarjanje na iztek.
- Rotacija ključev in certifikatov mora potekati najmanj vsaki dve leti oziroma po notranjih pravilih ali ob incidentu.
- Ob preklicu ali poteku veljavnosti mora biti zagotovljeno varno uničenje ali zamenjava ključa/certifikata.
- Vsi ključi in certifikati se morajo evidentirati v registru informacijskih sredstev in vključiti v oceno tveganj.

d) Digitalni podpisi in elektronska komunikacija

- Digitalni podpisi in certifikati se uporabljajo za zagotavljanje integritete, avtentičnosti in dokazljivosti izvora in pristnosti elektronskih transakcij, dokumentov in komunikacije.
- Digitalna potrdila mora izdati zaupanja vreden overitelj in imeti ustrezno dolžino ključa.
- Uporaba neoverjenih ali samopodpisanih certifikatov je dovoljena le za testna okolja in mora biti ustrezno označena.
- Za zaščito elektronske pošte se uporablja TLS, S/MIME ali PGP.

e) Pregled in skladnost

- Učinkovitost in skladnost uporabljenih kriptografskih mehanizmov se preverja najmanj enkrat letno.
- Pregled vključuje oceno ustreznosti algoritmov, dolžin ključev, postopkov rotacije in skladnosti s priporočili (npr. ENISA, NIST, URSIV).
- Ugotovljene pomanjkljivosti se morajo odpraviti v razumnem roku glede na tveganje.

f) Odgovornosti in skladnost

- Za izvajanje kriptografskih ukrepov in upravljanje ključev so odgovorni skrbniki sistemov v sodelovanju z vodjo informacijske varnosti[36].
- Vodja informacijske varnosti[37] skrbi za skladnost te politike z drugimi področnimi dokumenti (npr. politiko nadzora dostopa, politiko ravnanja s sredstvi, načrtom neprekinjenega poslovanja).
- Vse spremembe, ki vplivajo na uporabo kriptografskih mehanizmov ali algoritmov, morajo biti odobrene, dokumentirane in preverjene.

2.10 Politika zaščite pred zlonamerno programsko opremo

Politika zaščite pred zlonamerno programsko opremo določa tehnične in organizacijske ukrepe za preprečevanje, zaznavanje in odzivanje na zlonamerno kodo (ang. *malware*) v informacijskih

[36] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, je odgovornost neposredno na vodstvu.
[37] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za skladnost skrbi neposredno vodstvo.

sistemih organizacije. Namen politike je zmanjšati verjetnost okužb in njihov vpliv na razpoložljivost, zaupnost, celovitost in avtentičnost podatkov ter storitev organizacije.

a) Preprečevanje (preventiva)

- Vse končne naprave (strežniki, delovne postaje, prenosniki, mobilne naprave) morajo imeti nameščeno in posodobljeno zaščito pred zlonamerno programsko opremo z zaščito v realnem času in samodejnimi posodobitvami podpisov ter komponent.
- Kritični sistemi in strežniki morajo (kadar je izvedljivo) uporabljati EDR/XDR[38] z možnostjo izolacije, blokiranja in forenzičnega vpogleda.
- Na prehodih (e-pošta, splet, proxy/DNS) se uporabljajo filtri in pregled prilog/URL (AV/AM, reputacija, »sandboxing«).
- Strežniški in odjemalski OS in aplikacije morajo biti posodobljeni skladno s poglavjem 2.7 (upravljanje ranljivosti in posodobitev).
- Uveljavlja se načelo najmanjših privilegijev (brez lokalnih admin pravic za običajno delo).
- Uporablja se nadzor aplikacij (ang. *allowlisting* ali vsaj blokiranje znanih nevarnih tipov datotek/skript; omejitve za PowerShell/WSH – samo podpisani skripti, kjer je primerno).
- Brskalniki in pisarniška orodja morajo imeti uveljavljene varne nastavitve (onemogočeni makri iz interneta ali dovoljeni samo podpisani makri, zaščita pred nevarnimi prenosi).
- Omrežje je segmentirano; izhodni promet je omejen (ang. *egress filtering*) za zmanjšanje C2 komunikacij in omejevanje širjenja zlonamerne kode med segmenti.

b) Zaznavanje in odziv

- Orodja (AV/AM/EDR/XDR) morajo omogočati centralno upravljanje, nadzor in poročanje.
- Ob zaznavi visoko-tveganih dogodkov se izvede samodejna izolacija naprave (kjer je podprto) in odpre zahtevek v sistemu za obravnavo incidentov (če tak sistem obstaja; sicer se obvesti vodjo informacijske varnosti ali enoto, pristojno za IT).
- Po odpravi okužbe se izvede analiza vzroka in preverjanje, da ni ostankov zlonamerne kode ali stranskih učinkov (ang. *root-cause analysis in verification*).
- Odziv in poročanje morata biti skladno z načrtom odzivanja na incidente (notranji akt organizacije) in nacionalnim načrtom odzivanja na incidente (postopek prijave pristojnemu CSIRT).
- Redno se izvajajo načrtovani pregledi (ang. *full scan*) na končnih napravah in strežnikih.

[38] EDR/XDR - Endpoint Detection and Response / Extended Detection and Response - Zaznavanje in odziv na končnih točkah / Razširjeno zaznavanje in odziv.

c) e-pošta in spletna zaščita

- Za e-pošto se uporabljajo SPF, DKIM in DMARC (politika DMARC naj bo nastavljena najmanj na »quarantine«, priporočeno »reject«, ko je to možno).
- Na poštnih prehodih je omogočeno skeniranje in »sandboxing« prilog ter prepisovanje/analiza URL (ang. *safe links*).
- Privzeto so blokirane visoko rizične priloge (npr. .exe, .js, .vbs, makri v Office dokumentih iz interneta).
- Na spletnih prehodih ali DNS ravni se uporablja filtriranje reputacije in kategorij (blokada zlonamernih domen, C2, »phishing«).

d) Prenosni mediji in zunanji nosilci (USB, izmenljivi diski)

- Privzeto je onemogočena uporaba izmenljivih nosilcev na ključnih sistemih; dovoljeni so le predhodno odobreni in po potrebi šifrirani nosilci.
- Ob priklopu zunanjega nosilca na odobreni napravi se samodejno izvede skeniranje; funkcionalnost »AutoRun/AutoPlay« mora biti onemogočena.
- Za prenos podatkov med IT in OT okoljem se (kjer je primerno) uporabljajo prehodne (ang. *clean*) postaje z obveznim skeniranjem in zapisnikom prenosa.

e) Upravljanje orodij in konfiguracij

- Rešitve AV/AM/EDR/XDR[39] se upravljajo centralno; konfiguracije (politike) so standardizirane in dokumentirane.
- Posodobitve podpisov in komponent se izvajajo samodejno; za strežnike z visoko razpoložljivostjo se uporablja nadzorovan postopek.
- Sistemi morajo preverjati celovitost podpisnih datotek in komponent pred posodobitvijo (npr. digitalni podpis proizvajalca).
- Integracije z SIEM (ang. *security information and event management*) ali osrednjim dnevniškim sistemom se uvedejo, kadar so smiselne in izvedljive; minimalno se hranijo dogodki o zaznavah, izolacijah, izbrisanih grožnjah in neuspehih.

f) Ozaveščanje in usposabljanje

- Uporabniki se redno usposabljajo o prepoznavanju *phishinga*, nevarnih priponk, lažnih strani in pravilnem ravnanju z nosilci (del programa ozaveščanja in usposabljanja informacijske varnosti).
- Skrbniki in IKT osebje se stalno strokovno usposabljajo glede novih taktik in orodij (glej 2.1 politika ozaveščanja in usposabljanja).

g) Spremljanje, poročanje in kazalniki

- Organizacija spremlja naslednje kazalnike in mesečno poroča vodji informacijske varnosti[40]:
  - število zaznanih in blokiranih zlonamernih dogodkov;
  - MTTI/MTTR (čas do zaznave in izolacije / čas do popolne rešitve);
  - delež naprav z aktualno zaščito in uspešno posodobljenimi podpisnimi datotekami;
  - delež e-pošte, zavrnjene po SPF/DKIM/DMARC in

[39] AV/AM/EDR/XDR - AV – Antivirus, AM – Antimalware, EDR – Endpoint Detection and Response, XDR – Extended Detection and Response.
[40] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, se poroča neposredno vodstvu.

  - število incidentov, povezanih z USB/prenosnimi mediji.
- Neskladnosti in ponavljajoče se težave se naslovijo s korektivnimi ukrepi (tehničnimi ali procesnimi).

h) Odgovornost in skladnost

- Skrbniki sistemov in organizacijska enota, pristojna za IT so odgovorni za upravljanje orodij, odziv, poročanje o incidentih in za izvedbo korektivnih ukrepov po incidentih.
- Vodja informacijske varnosti skrbi za skladnost te politike z drugimi področnimi dokumenti (2.3 nadzor dostopa, 2.6 fizična in okoljska varnost, 2.7 ranljivosti, 2.8 varnostno kopiranje, načrt odzivanja na incidente).
- Spremembe konfiguracij in uvedbe novih zaščit morajo biti izvedene skladno s postopki upravljanja sprememb.

2.11 Politika neprekinjenega poslovanja in obvladovanja nesreč

Politika neprekinjenega poslovanja in obnovitve po nesreči določa okvir SUNP (BCMS), s katerim organizacija zagotavlja nadaljevanje ključnih storitev med in po motnji ter obnovitev IKT sistemov po izpadu ali katastrofi. Politika temelji na analizi vpliva na poslovanje (BIA) in vključuje pripravo ter vzdrževanje načrta neprekinjenega poslovanja (BCP) in načrta obnovitve po nesreči (DRP).

a) Namen in obseg

- Politika zajema vse kritične poslovne procese in pripadajoče informacijske sisteme, podatke, prostore, osebje in ključne dobavitelje.
- Načrt neprekinjenega poslovanja določa, kako organizacija nadaljuje poslovanje v času motnje.
- Načrt obnovitve in ponovne vzpostavitve določa, kako se obnovijo IKT sistemi in podatki po izpadu ali napadu.
- Oba načrta temeljita na rezultatih analize vpliva na poslovanje in oceni tveganj.

b) Ključni elementi načrtovanja

- V oceni vplivov na poslovanje organizacija določi kritične procese, odvisnosti, ključne vire ter cilje RTO (čas obnove) in RPO (točka obnove).
- Načrt neprekinjenega poslovanja in načrt obnovitve in ponovne vzpostavitve sistemov morata vključevati:
  - vloge in odgovornosti ob motnjah;
  - postopke aktivacije in obveščanja;
  - komunikacijske poti (zaposleni, dobavitelji, CSIRT, regulatorji);
  - postopke za obnovitev ključnih storitev in sistemov in
  - kontaktne sezname in nadomestne lokacije (če obstajajo).
- Za vsak ključni proces se določijo možne nadomestne rešitve ali začasni postopki dela, ki omogočajo izvajanje osnovnih funkcij do popolne obnove sistema.

c) Preizkušanje in posodabljanje

- Načrti neprekinjenega poslovanja in načrti obnovitve in ponovne vzpostavitve se preverjajo najmanj enkrat letno ali po vsaki večji spremembi v sistemih, procesih ali organizaciji.
- Preizkusi vključujejo vaje odzivanja in test obnovitve iz varnostnih kopij.

- Po vsaki vaji ali dejanski uporabi se izvede ocena uspešnosti in po potrebi posodobitev načrtov.

d) Komunikacija in sodelovanje

- Organizacija mora zagotoviti postopke za obveščanje notranjih in zunanjih deležnikov v primeru motnje (zaposleni, partnerji, javnost, regulatorji).
- če organizacija uporablja zunanje izvajalce ali storitve v oblaku, morajo pogodbe vključevati obveznost izvajalcev, da zagotavljajo lastne postopke za neprekinjeno poslovanje in obnovo.

e) Odgovornosti in skladnost

- Vodstvo potrdi politiko in zagotavlja vire za izvajanje načrta neprekinjenega poslovanja in načrta obnovitve in ponovne vzpostavitve sistemov.
- Vodja informacijske varnosti[41] skrbi za usklajenost te politike z drugimi področnimi dokumenti (2.6 fizična in okoljska varnost, 2.7 ranljivosti, 2.8 varnostno kopiranje),
- Lastniki procesov sodelujejo pri pripravi in testiranju načrtov.
- Vsi zaposleni morajo biti seznanjeni s svojimi nalogami v primeru motnje.

Za učinkovito izvajanje neprekinjenega poslovanja se politika uporablja skupaj z **obema načrtoma**:				
Načrt	**Angleški izraz**	**Namen**	**Obseg**	**Primeri vsebine**
Načrt neprekinjenega poslovanja	Business Continuity Plan (BCP)	Zagotavlja nadaljevanje izvajanja ključnih poslovnih funkcij med motnjo in po njej.	Širok – vključuje procese, prostore, komunikacijo, kadre in dobavitelje.	Vloge in odgovornosti, krizna komunikacija, nadomestne lokacije, postopki za nadaljevanje dela.
Načrt obnovitve po nesreči	Disaster Recovery Plan (DRP)	Zagotavlja obnovitev IT sistemov, aplikacij in podatkov po izpadu.	Ožji – osredotočen na IT in infrastrukturo.	Postopki za obnovitev strežnikov, omrežij, aplikacij in podatkov, RTO in RPO cilji, vrstni red obnovitve.

2.12 Politika spremljanja in evidentiranja revizijskih sledi

Politika spremljanja in evidentiranja revizijskih sledi določa način beleženja, hranjenja in pregleda dogodkov v informacijskih sistemih, da se zagotovi sledljivost dejanj, pravočasno zaznavanje incidentov in podpora preiskavam varnostnih dogodkov.

[41] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za skladnost skrbi neposredno vodstvo.

a) Obseg in namen beleženja

- Beleženje obsega vse pomembne dogodke v informacijskih sistemih, kot so prijave, dostopi, spremembe pravic, nastavitev ali konfiguracij, posodobitve in nadgradnje ter obdelave občutljivih podatkov.
- Vsi ključni informacijski sistemi, aplikacije in omrežna oprema morajo omogočati beleženje dogodkov.
- Dnevniški zapisi obsegajo najmanj:
  - izhodni in vhodni omrežni promet;
  - ustvarjanje, spreminjanje ali brisanje uporabnikov omrežnih in informacijskih sistemov zadevnih subjektov ter razširitev dovoljenj;
  - dostop do sistemov, aplikacij in baz podatkov;
  - dogodke, povezane z avtentikacijo;
  - vse privilegirane dostope do sistemov in aplikacij ter dejavnosti, ki jih izvajajo upraviteljski računi;
  - dostop ali spremembe kritičnih konfiguracijskih in varnostnih datotek;
  - zapise dogodkov in zapise iz varnostnih orodij, kot so protivirusni programi, sistemi za odkrivanje vdorov ali požarni zidovi;
  - uporabo sistemskih virov in njihovo zmogljivost;
  - dostop do omrežne opreme in naprav ter njihovo uporabo in
  - aktiviranje, zaustavitev in prekinitev sistemskih storitev in beleženja zapisov.
- Aktivnosti skrbnikov se beležijo ločeno od običajnih uporabniških dejanj (npr. z uporabo »audit logginga« ali ločenih revizijskih sledi)[42].
- Dnevniki dogodkov morajo vsebovati podatke o uporabniku, času, izvoru, cilju in rezultatu dejavnosti.

b) Sinhronizacija časa

- Vsi sistemi morajo uporabljati usklajene in preverjene časovne vire (protokol NTP).
- Usklajen čas je pogoj za pravilno zaporedje in korelacijo dogodkov med različnimi sistemi.
- Za varnost NTP protokola se uporabljajo varnejše rešitve (npr. ntpsec, Chrony, javni NTS strežniki) ali notranji NTP strežnik, dostopen le z zaupanja vrednih naslovov.
- Vključeno mora biti beleženje NTP dogodkov, zlasti anomalij (npr. časovni preskoki).

c) Pregledovanje in obveščanje

- Dnevniki dogodkov se redno (najmanj tedensko) pregledujejo, s poudarkom na ključnih sistemih in upravljavskih računih.
- V primeru zaznave sumljivih dejavnosti se o tem takoj obvesti vodjo informacijske varnosti[43] ali pooblaščeno osebo.
- Če sistem podpira samodejno obveščanje o varnostnih dogodkih, je ta funkcionalnost omogočena.

[42] Skrbniki (ang. administrators, root, domain admin, DBA, network admin ipd.) imajo najvišje privilegije v sistemu — in s tem tudi možnost, da sami (ali nekdo, ki je nepooblaščeno pridobil njihove pravice) spremenijo ali izbrišejo dokaze o lastnih dejanjih, spremenijo varnostne nastavitve, uporabnike ali pravice, namestijo ali odstranijo programsko opremo ali celo izklopijo ali manipulirajo z beleženjem. Njihove aktivnosti je treba zato beležiti v ločen sistem ali ločeno revizijsko sled, do katere nimajo dostopa.
[43] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan.

d) Centralizacija in orodja

- Organizacija mora zagotoviti, da so dnevniki shranjeni na varnem mestu in zaščiteni pred brisanjem ali spremembami.
- Kadar je mogoče, se uporablja centraliziran zbiralnik dnevnikov ali orodje za spremljanje dogodkov.
- Če uporaba naprednega sistema za upravljanje varnostnih dogodkov (SIEM) ni izvedljiva, organizacija zagotovi drugo ustrezno rešitev, ki omogoča pregled in arhiviranje dnevnikov (npr. odprtokodni ali brezplačni zbiralnik dnevnikov).

e) Hramba in varovanje

- Dnevniki se hranijo najmanj 12 mesecev (lahko tudi dlje, če to izhaja in ocene tveganj).
- Dostop do dnevnikov je omejen na pooblaščene osebe.
- Za dnevnike, ki vsebujejo osebne podatke, veljajo določbe predpisov s področja varstva osebnih podatkov.
- Dnevniki morajo biti zaščiteni pred nepooblaščenim posegom tako, da se zagotovi njihova avtentičnost, celovitost in razpoložljivost (tudi v primeru incidentov).
- Vsebine dnevnikov ni dovoljeno brisati (razen po poteku zakonsko določenega roka), potvarjati ali kako drugače spreminjati.

f) Odgovornost in skladnost

- Skrbniki sistemov so odgovorni za pravilno delovanje beleženja in redni pregled dnevnikov.
- Vodja informacijske varnosti[44] skrbi za skladnost te politike z drugimi področnimi dokumenti (npr. politiko nadzora dostopa, politiko zaščite pred zlonamerno programsko opremo in načrtom odzivanja na incidente).
- Ugotovljene neskladnosti ali pomanjkljivosti se morajo odpraviti v razumnem roku, o rezultatih pregledov pa se poroča vodstvu.
- Geografska lokacija hrambe dnevniških zapisov mora biti skladna z ZInfV-1.

2.13 Politika uporabe IKT sredstev

Politika uporabe IKT sredstev določa pravila za varno in odgovorno uporabo informacijskih naprav, sistemov in programske opreme v organizaciji. Namen politike je preprečiti zlorabe, ohraniti razpoložljivost in celovitost sistemov ter zaščititi podatke organizacije.

a) Obseg

- Politika velja za vse zaposlene, pogodbenike in zunanje sodelavce, ki uporabljajo službene naprave ali dostopajo do informacijskih sistemov organizacije.
- Nanaša se na namizne in prenosne računalnike, mobilne naprave, strežnike, omrežno opremo in pripadajočo programsko opremo.

b) Osnovna varnostna pravila

- Prepovedano je odstranjevanje ali onemogočanje zaščitnih mehanizmov (npr. protivirusne zaščite, požarnih zidov, sistemov EDR/XDR).

[44] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za skladnost skrbi neposredno vodstvo.

- Programska in strojna oprema morata biti redno posodabljani, skladno s politiko 2.7 (upravljanje ranljivosti in posodobitev).
- Diskovno šifriranje je obvezno na prenosnih računalnikih in drugih prenosnih napravah (glej politiko 2.9 kriptografije).
- Uporabniki ne smejo nameščati neodobrene programske opreme ali spreminjati nastavitev sistemov brez dovoljenja skrbnikov.
- Vsaka naprava, ki dostopa do omrežij ali podatkov organizacije, mora imeti aktivno zaščito pred zlonamerno programsko opremo (glej politiko 2.10 zaščite pred zlonamerno programsko opremo).

c) Uporaba naprav

- Službene naprave se uporabljajo izključno za poslovne namene; osebna raba je dovoljena le, če ne ogroža varnosti.
- Uporabniki morajo zagotoviti fizično varnost naprav – preprečiti odtujitev, nepooblaščen dostop ali opustitev naprave brez nadzora.
- V primeru izgube, kraje ali suma zlorabe mora uporabnik dogodek nemudoma prijaviti pristojnemu oddelku, v primeru, da gre za ključno sredstvo, pa tudi vodji informacijske varnosti[45].
- Prenosni mediji (USB-ključki, zunanji diski) se lahko uporabljajo le, če:
  - jih uporabniku izda organizacija ali
  - če so predhodno odobreni in preverjeni na zlonamerno kodo.

d) Elektronska komunikacija

- Elektronska pošta in spletne storitve se uporabljajo odgovorno in v poslovne namene, prepovedano je pošiljanje neprimernih, žaljivih ali zlonamernih vsebin.
- Uporabniki ne smejo odpirati sumljivih prilog ali povezav ter morajo takšne primere prijaviti pristojni enoti.
- Varnostni mehanizmi (SPF, DKIM, DMARC, filtriranje prilog/URL) so vzpostavljeni na ravni poštnih prehodov (glej politiko 2.10 zaščite pred zlonamerno programsko opremo).

e) Izločanje in uničenje sredstev

- Pred izločitvijo naprave iz uporabe mora biti zagotovljeno varno brisanje podatkov ali fizično uničenje nosilca.
- O izvedenem postopku se vodi evidenca, skladno s politiko 2.4 (ravnanje s sredstvi).

f) Odgovornost in skladnost

- Uporabniki so odgovorni za varno uporabo naprav in spoštovanje te politike.
- Skrbniki sistemov zagotavljajo tehnično podporo, nadzor nad skladnostjo in izvajajo ukrepe za preprečevanje zlorab.
- Vodja informacijske varnosti[46] skrbi za skladnost politike z drugimi področnimi dokumenti (2.7, 2.9, 2.10, 2.4) in za ozaveščanje uporabnikov o pravilni uporabi IKT sredstev.

[45] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan.
[46] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za skladnost skrbi neposredno vodstvo.

2.14 Politika uporabe oblačnih storitev

Politika uporabe oblačnih storitev določa pravila za varno izbiro, uporabo in nadzor oblačnih rešitev, ki jih uporablja organizacija. Namen politike je zagotoviti, da so podatki in storitve v oblačnih okoljih zaščiteni, skladni z zakonodajo ter da organizacija ohranja nadzor nad informacijami, ki jih zaupa ponudnikom oblačnih storitev.

Varnost v oblačnih okoljih temelji na načelu deljene odgovornosti (ang. *shared responsibility model*): ponudnik zagotavlja varnost infrastrukture, organizacija pa je odgovorna za zaščito svojih podatkov, uporabniških računov in konfiguracij.

a) Obseg

- Politika velja za vse oblačne storitve, ki jih organizacija uporablja za poslovne namene (npr. shranjevanje podatkov, e-pošta, sodelovanje, gostovanje, varnostno kopiranje).
- Nanaša se na modele javnega, zasebnega in hibridnega oblaka ter storitvene modele IaaS, PaaS in SaaS.

b) Izbor ponudnika in pogodbeni pogoji

- Oblačne storitve se smejo uporabljati le, če ponudnik izpolnjuje varnostne in skladnostne zahteve organizacije, vključno z dokazili o skladnosti (npr. ISO/IEC 27001, ISO/IEC 27017, SOC 2 Type II, CSA STAR).
- Pred sklenitvijo pogodbe se izvede ocena tveganja, ki jo potrdi vodja informacijske varnosti[47] ali vodstvo.
- Ponudnik mora na zahtevo organizacije predložiti dokazila o rednih varnostnih presojah ali objavljati poročila o skladnosti. Če so ta poročila javno dostopna, jih organizacija sama redno pregleduje in hrani dokaze o pregledu.
- Pogodba mora vključevati najmanj:
  - določitev kraja hrambe podatkov (z upoštevanjem omejitev iz GDPR, ZVOP-2, ZInfV-1);
  - pravico organizacije do vpogleda v varnostna poročila ali rezultate presoj;
  - obveznost ponudnika pravočasnega obveščanja o varnostnih incidentih;
  - ukrepe za zaščito podatkov, vključno s šifriranjem, varnostnimi kopijami in postopki ob prenehanju pogodbe;
  - postopke vračanja ali izbrisa podatkov po prekinitvi sodelovanja in
  - možnost izdelave kopije vseh podatkov v formatu, ki organizaciji omogoča prenos teh podatkov k drugemu ponudniku v primeru prekinitve pogodbe z obstoječim ponudnikom.
- Ponudnik mora zagotavljati redne varnostne posodobitve, odpravljati ugotovljene ranljivosti in objavljati ali na zahtevo organizacije posredovati poročila o odpravljenih ranljivostih.
- Organizacija mora periodično preverjati uporabo vseh aktivnih oblačnih storitev in zaznavati neodobrene (ang. *shadow IT*) račune ali aplikacije.
- Organizacija najmanj enkrat letno preveri skladnost ponudnika z zahtevanimi varnostnimi standardi.

[47] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan.

c) Dostop in upravljanje

- Dostop do oblačnih storitev mora temeljiti na načelu najmanjšega privilegija in biti zaščiten z večfaktorsko avtentikacijo.
- Uporabniki morajo uporabljati službene uporabniške račune in ne osebnih e-poštnih ali oblačnih računov.
- Pri uporabi več oblačnih okolij mora organizacija uveljaviti enotne standarde varnostnih nastavitev in politik.
- Odstranjevanje ali deljenje računov brez odobritve skrbnika je prepovedano.
- Pristojna organizacijska enota najmanj enkrat letno preveri ustreznost vseh dostopov.

d) Varovanje podatkov

- Vsi podatki, ki se prenašajo v ali iz oblačnih okolij, morajo biti šifrirani pri prenosu in v mirovanju skladno s poglavjem 2.9 Politika kriptografije.
- Če je mogoče, organizacija uporablja storitve, ki omogočajo šifriranje ključev pod njenim nadzorom (ang. *Customer Managed Keys – CMK*).
- Kadar organizacija sama upravlja aplikacije ali podatkovne zbirke v oblaku (npr. PaaS ali IaaS), mora zagotoviti samodejno posodabljanje in odpravljanje ranljivosti skladno s poglavjem 2.7 politika upravljanja z ranljivostmi in posodobitvami.
- Poslovni podatki se ne smejo deliti z javnimi ali neodobrenimi oblačnimi storitvami.
- Uporabniki ne smejo sinhronizirati ali kopirati poslovnih podatkov v zasebne oblačne račune ali naprave (prepoved "*shadow IT*").

e) Beleženje in spremljanje

- Vse pomembne aktivnosti v oblačnih storitvah (prijave, spremembe, prenos podatkov, administrativna dejanja) morajo biti beležene skladno s poglavjem 2.12 Politika spremljanja in evidentiranja revizijskih sledi.
- Ponudnik mora omogočati vpogled in izvoz revizijskih dnevnikov (ang. *audit logs*), ki vključujejo najmanj podatke iz poglavja 2.12 Politika spremljanja in evidentiranja revizijskih sledi.
- Dnevniki se morajo hraniti najmanj 12 mesecev in biti zaščiteni pred spremembami ali brisanjem.

f) Upravljanje incidentov in izhodna strategija

- Ponudnika se s pogodbo zaveže k spoštovanju postopkov in rokov za odzivanje na incidence iz Načrta odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT.
- Organizacija mora imeti opredeljene postopke za prenos, izvoz ali brisanje podatkov ob prenehanju uporabe storitve.
- Pred prenosom na novega ponudnika mora organizacija:
  - preveriti celovitost in razpoložljivost podatkov;
  - od obstoječega ponudnika zahtevati kopijo podatkov v formatu, ki omogoča prenos k novemu ponudniku in
  - izbrisati prejšnje kopije oziroma od ponudnika zahtevati dokazilo ali potrdilo o uničenju.

g) Odgovornosti in skladnost

- Vodstvo potrdi uporabo oblačnih storitev ter zagotavlja potrebne vire za ocenjevanje, pogodbeno ureditev in nadzor skladnosti.
- Vodja informacijske varnosti[48] je odgovoren za preverjanje skladnosti ponudnikov in izvajanje ocen tveganja.
- Skrbniki sistemov zagotavljajo ustrezno konfiguracijo in pregled dostopov.
- Uporabniki so odgovorni za varno rabo oblačnih storitev in spoštovanje določb te politike.

2.15 Politika uporabe brezžičnih omrežij

Politika uporabe brezžičnih omrežij določa pravila in tehnične zahteve za varno zasnovo, uporabo in nadzor brezžičnih (ang. *Wi-Fi*) povezav v organizaciji. Namen politike je preprečiti nepooblaščen dostop, zmanjšati izpostavljenost grožnjam in zagotoviti zanesljivo ter varno brezžično povezljivost za zaposlene in obiskovalce.

a) Osnovne zahteve

- Vsa brezžična omrežja morajo biti zaščitena z močnim geslom in sodobnim varnostnim protokolom (najmanj WPA2-Enterprise ali WPA2-PSK, priporočeno WPA3).
- Uporaba zastarelih ali ranljivih protokolov (npr. WEP, WPA, WPS) je prepovedana.
- Privzeta administratorska gesla in nastavitve dostopnih točk morajo biti spremenjene pred uporabo.
- Dostopne točke in njihova programska oprema (ang. *firmware*) morajo biti redno posodabljane.
- Brezžične naprave in dostopne točke morajo biti fizično zaščitene pred nepooblaščenim posegom.

b) Segmentacija in izolacija omrežij

- Omrežje mora biti razdeljeno najmanj na dve ločeni coni:
  - poslovno omrežje, namenjeno zaposlenim in službenim napravam, ter
  - gostujoče omrežje, namenjeno obiskovalcem.
- Poslovno omrežje mora biti ločeno tudi od morebitne IoT-cone (npr. tiskalniki, kamere, pametne naprave).
- Gostujoče omrežje mora biti popolnoma izolirano od poslovnega in omogočati le dostop do interneta.
- Naprave zaposlenih ne smejo dostopati do gostujočega omrežja.
- Dostop do gostujočega omrežja se zagotavlja prek časovno omejenih (voucher) gesel ali dnevnih gesel; stalna skupna gesla niso dovoljena.
- V gostujočem omrežju mora biti onemogočena P2P komunikacija, pasovna širina pa omejena glede na potrebe.
- Na vseh omrežjih se priporoča uporaba DNS filtriranja za blokiranje zlonamernih domen.

c) Dostop in upravljanje

- Dostop do poslovnega omrežja je dovoljen samo odobrenim napravam, ki so evidentirane v registru sredstev ali jih odobri pristojna oseba ali enota.
- Odobrene naprave morajo izpolnjevati minimalne varnostne zahteve (posodobljen operacijski sistem, protivirusna zaščita, šifriran disk).

[48] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za te naloge skrbi neposredno vodstvo.

- Avtentikacija uporabnikov in naprav mora temeljiti na centralnem nadzoru (npr. RADIUS, 802.1X) ali drugem preverljivem mehanizmu.
- Vsi dostopi do brezžičnih omrežij se beležijo, najmanj z navedbo časa, uporabnika in naprave, skladno s poglavjem 2.12 (Politika spremljanja in evidentiranja revizijskih sledi).
- V primeru zaznane sumljive dejavnosti (npr. poskus prijave neznane naprave) mora sistem sprožiti obvestilo pristojni enoti.

d) Spremljanje in preverjanje

- Brezžična omrežja in dostopne točke morajo biti vključene v logično shemo omrežja in nadzorovana prek centralnega sistema.
- Vzpostavljen mora biti protokol rednega spremljanja (monitoringa) in opozarjanja ob zaznavi nenavadnih dogodkov ali nepooblaščenih dostopnih točk (ang. *rogue AP*).
- O zaznanih nepooblaščenih dostopnih točkah ali poskusih povezave pristojna oseba ali enota pripravi poročilo in ukrep dokumentira skladno s postopkom obravnave incidentov.
- Najmanj enkrat letno se izvede pregled konfiguracij, revizija gesel in iskanje nepooblaščenih točk ali povezav.
- Vsi rezultati pregledov se dokumentirajo, odstopanja pa se odpravijo v dogovorjenem roku.

e) Odgovornosti in skladnost

- Skrbniki omrežij so odgovorni za pravilno konfiguracijo, segmentacijo, posodobitve in spremljanje dostopnih točk.
- Uporabniki so odgovorni za varno uporabo brezžičnega dostopa in poročanje o morebitnih težavah ali sumljivih povezavah.
- Vodja informacijske varnosti[49] skrbi za skladnost te politike z drugimi področnimi dokumenti (2.7 upravljanje z ranljivostmi, 2.10 zaščita pred zlonamerno programsko opremo, 2.12 revizijske sledi).

2.16 Politika dela od doma in na oddaljenih lokacijah

Politika dela od doma ali z druge oddaljene lokacije določa pravila in tehnične zahteve za varen dostop zaposlenih do informacijskih sistemov organizacije izven poslovnih prostorov. Namen politike je zagotoviti, da delo na daljavo poteka varno, da so podatki in sistemi zaščiteni ter da se zmanjšajo tveganja, povezana s povečanjem napadena površine.

a) Obseg

- Politika velja za vse zaposlene, pogodbenike in zunanje sodelavce, ki dostopajo do informacijskih sistemov organizacije izven poslovnih prostorov.
- Delo od doma ali na oddaljeni lokaciji je dovoljeno le ob predhodnem soglasju vodje oziroma pooblaščene osebe in ob upoštevanju varnostnih zahtev organizacije.

[49] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za te naloge skrbi neposredno vodstvo.

b) Dostop in povezave

- Oddaljeni dostopi do sistemov organizacije morajo potekati izključno prek zaščitene povezave – npr. VPN ali drug varni dostopni kanal, ki zagotavlja šifrirano povezavo.
- Uporaba protokolov in kriptografskih nastavitev mora temeljiti na sodobnih in preverjenih standardih (npr. WireGuard, OpenVPN, IKEv2/IPsec z AES-256, ChaCha20, SHA-2/384/512 in Diffie-Hellman skupinami, npr. DH 3072+, oziroma njihovimi nasledniki).
- Dostop mora biti zaščiten z večfaktorsko avtentikacijo.
- Uporabljajo se lahko le odobrene in zaščitene naprave (npr. prenosniki organizacije ali osebne naprave pod nadzorom – ang. *MDM*, kjer so omogočene varnostne nastavitve, posodobljeni operacijski sistem, šifriranje diska in zaščita pred zlonamerno kodo).
- Pri delu izven poslovnih prostorov mora biti zagotovljeno varno delovno okolje, ki preprečuje dostop nepooblaščenim osebam do naprav ali informacij (npr. fizična varnost, zasebni prostor, naprava ni brez nadzora).
- Uporabnik poslovnih podatkov doma ali na lokacijah, ki niso pod neposrednim nadzorom organizacije, ne sme tiskati, kopirati ali izven varnega kanala prenašati poslovnih podatkov ali jih puščati brez nadzora.

c) Uporaba in omejitve

- Shranjevanje poslovnih podatkov na osebne naprave, na neodobrene zunanje pomnilnike ali v neodobrene oblačne storitve je prepovedano, razen če shranjevanje skladno s politiko organizacije dovoli pristojna oseba ali enota.
- Naprave, s katerimi uporabniki oddaljeno dostopajo do sistemov organizacije, morajo imeti vključeno zaklepanje zaslona po določenem času neaktivnosti (npr. največ 5 min).
- Uporabniki morajo napravo ročno zaklepati, če ni v njihovem neposrednem nadzoru (npr. začasen odhod iz prostora, kjer je naprava).
- Uporabnik ne sme omogočiti deljenja naprave, uporabe uporabniškega računa drugih ali omogočiti dostopa nepooblaščenim osebam.

d) Nadzor, pregled in obveščanje

- Uporabniki morajo vse incidenti ali vsa sumljiva dogajanja, povezana z delom na daljavo ali oddaljenih lokacijah, nemudoma prijaviti skladno s točko 1.7 upravljanje incidentov in v skladu z notranjim načrtom odzivanja na incidente.
- Pristojna oseba ali enota redno preverja dostope iz oddaljenih lokacij (npr. pregled, ali naprava, ki se povezuje, izpolnjuje varnostne zahteve).

e) Odgovornosti in skladnost

- Vodja informacijske varnosti je odgovoren za določitev varnostnih zahtev za delo na daljavo, nadzor izvajanja te politike in pregled skladnosti z drugimi dokumenti (npr. 2.7 Upravljanje z ranljivostmi in posodobitvami, 2.10 Zaščita pred zlonamerno programsko opremo, 2.12 Revizijske sledi).
- Organizacijska enota, pristojna za IT infrastrukturo, je odgovorna za vzpostavitev in vzdrževanje infrastrukture za varen oddaljen dostop, za izdajo pooblastil, nadzor naprav in njihovo skladnost.
- Zaposleni in pogodbeni sodelavci so odgovorni za prilagoditev svoje domače ali oddaljene delovne površine ter za spoštovanje določb te politike – zlasti za varno ravnanje z napravami in podatki.

2.17 Politika čiste mize in zaklepanja zaslona

Politika čiste mize in zaklepanja zaslona določa minimalna pravila, s katerimi organizacija zmanjšuje tveganje nenamernega razkritja informacij v pisarnah, na skupnih površinah in pri delu v bližini tretjih oseb.

a) Obseg

- Politika velja za vse zaposlene, pogodbene in zunanje sodelavce v prostorih organizacije ter – kjer je smiselno – pri delu na domu ali oddaljenih lokacijah (glej 2.16).

b) Čista miza (ob vsakem odhodu in ob koncu dneva)

- Ob vsaki odsotnosti z delovnega mesta (sestanek, malica ipd.) mora uporabnik odstraniti ali zakriti dokumente s poslovnimi podatki in nosilce, ki jih vsebujejo (USB, zunanji diski, ključi).
- Ob koncu delovnega dne v delovnem okolju uporabnika ne sme biti vidnih dokumentov, prenosnih nosilcev, izpisov, zapiskov z občutljivimi podatki in vključenih naprav.
- Fizični dokumenti in drugi nosilci se med odsotnostjo uporabnika hranijo v zaklenjenih omarah/predalih.

c) Zaklepanje zaslona

- Uporabnik mora ročno zakleniti zaslon ob vsaki odsotnosti z delovnega mesta.
- Samodejno zaklepanje zaslona se nastavi na največ 5 minut neaktivnosti.
- Kjer je izvedljivo, se uporabljajo zaslonske pregrade (Ang. *privacy screen*) v odprtih prostorih ali pri delu z osebnimi/občutljivimi podatki.

d) Tiskanje, izpisi in beležke

- Fizični izvodi dokumentov se tiskajo samo, kadar je nujno potrebno; uporabnik mora izpise takoj prevzeti s tiskalnika.
- Prepisani/*wipeboard* zapiski s poslovno občutljivo vsebino se po sestanku izbrišejo; fotozajem tabel je dovoljen le z izrecnim dovoljenjem organizacije.
- Dokumente, ki jih uporabnik ne potrebuje več ter neuporabljene osnutek dokumentov uporabnik nemudoma uniči z rezalnikom ustreznega razreda (odvisno od občutljivosti podatkov, ki jih dokument vsebuje).

e) Varnost prenosnih medijev, naprav in dokumentov

- Kadar prenosni mediji, naprave organizacije ali dokumenti s poslovnimi podatki niso v prostorih organizacije, jih mora imeti uporabnik pod neposrednim nadzorom ali zaklenjene; ni jih dovoljeno puščati v vozilih, na vidnih mestih ali drugače brez nadzora.
- Naprav in dokumentov iz prejšnjih alinej tudi ni dovoljeno puščati v sejnih sobah in drugih prostorih, ki niso izključno namenjeni poslovanju organizacije.
- Po sestankih morajo uporabniki odstraniti gradivo z miz in zaslonov ter izključiti projektorje in zaslone.
- Obiskovalce mora ves čas spremljati zaposleni v organizaciji; med obiskom ne smejo imeti vidnega dostopa do poslovno občutljivih informacij.

f) Odgovornosti in skladnost

- Vsak uporabnik je odgovoren za čisto mizo in zaklep zaslona na svojem delovnem mestu.
- Vodstvo zagotavlja ustrezna mesta za hrambo prenosnih medijev, naprav in dokumentov.
- Vodje enot zagotavljajo, da uporabniki v enotah izvajajo to politiko; kršitve se obravnavajo skladno z delovno pravnimi predpisi.
- Vodja informacijske varnosti skrbi za skladnost te politike z ostalimi področnimi dokumenti.

3. Izvajanje in nadzor

Cilj izvajanja in nadzora politike informacijske varnosti je zagotoviti, da organizacija deluje skladno z zahtevami zakonodaje (ZInfV-1, ZVOP-2, GDPR in drugi predpisi) ter notranjimi politikami, da redno preverja učinkovitost tehničnih in organizacijskih ukrepov v skladu z načrtom varnostnih ukrepov in da stalno izboljšuje svoj sistem upravljanja varovanja informacij (SUVI) in sistem upravljanja neprekinjenega poslovanja (SUNP).

3.1 Zakonodajna skladnost in obveščenost

Organizacija mora spremljati in zagotavljati skladnost z vsemi veljavnimi predpisi, standardi in pogodbenimi obveznostmi, ki urejajo informacijsko in kibernetsko varnost, varstvo osebnih podatkov ter neprekinjeno poslovanje. Vsi zaposleni, zunanji sodelavci in vodstvo se morajo redno seznanjati s spremembami zakonodaje, ki vplivajo na njihovo delo. Vodja informacijske varnosti skrbi za sprotno obveščanje vodstva o spremembah zakonodaje, ki zahtevajo spremembo notranjih politik ali postopkov.

3.2 Izvajanje ukrepov

Pri izvajanju varnostnih ukrepov in nadzora mora podjetje upoštevati pristop, ki temelji na tveganju, in zagotavljati zadostne vire za podporo neprekinjenemu izboljševanju varnostnega okvira. Ukrepi morajo ustrezati kriterijem iz 22. člena ZInfV-1. Morajo se morajo redno pregledovati glede na spremembe v tehnologiji, poslovanju, predpisih ali ugotovljenih ranljivostih in incidentih.

Izvajati se mora presoja učinkovitosti varnostnih ukrepov v skladu z internim aktom *Politika s postopki za oceno učinkovitosti varnostnih ukrepov* .

3.3 Preverjanje skladnosti in presoje

Notranje presoje ali samoocene skladnosti se izvajajo najmanj vsakih 24 mesecev ali pogosteje, če to zahtevajo spremembe zakonodaje, tehnologije ali ocene tveganj. Presoja obsega skladnost z notranjimi politikami, zakonskimi zahtevami in standardi ter učinkovitost izvedenih ukrepov. Izvajajo jo usposobljene osebe, ki so neodvisne od presojanega področja, skladno z načelom nepristranskosti.

Kadar to zahtevajo regulatorji ali pogodbeni pogoji, se izvede tudi zunanja presoja (npr. po ISO/IEC 27001 ali na zahtevo pristojnega nadzornega organa).

Rezultati presoj se dokumentirajo, neskladnosti pa se odpravljajo v razumnem roku glede na resnost tveganja.

3.4 Merjenje in ocena učinkovitosti ukrepov

Organizacija mora vzpostaviti in dokumentirati postopke za preverjanje učinkovitosti tehničnih in organizacijskih ukrepov, vključno z vzorčnim preverjanjem, testiranjem, revizijami in ocenjevanjem varnostnih kontrol.

Rezultati ocenjevanja se uporabljajo za izboljšanje obstoječih politik, postopkov in varnostnih kontrol. Izvajanje ocene učinkovitosti poteka v skladu z internim aktom Politika s postopki za oceno učinkovitosti varnostnih ukrepov.

3.5 Poročanje, dokumentacija in sledljivost

Rezultati presoj, testov, analiz in ocenjevanj se hranijo kot dokazi o skladnosti. Vsa poročila morajo biti pregledna, podpisana in dostopna vodstvu.

Vodja informacijske varnosti[50] najmanj enkrat letno pripravi poročilo vodstvu o stanju varnosti, skladnosti in učinkovitosti ukrepov ter predlaga izboljšave.

Vodstvo preuči poročila in sprejme odločitve o potrebnih korektivnih ukrepih, dodatnih virih ali posodobitvah politik.

Na podlagi ugotovitev presoj, incidentov in sprememb tveganj organizacija stalno izboljšuje svoj sistem varovanja informacij.

3.6 Odgovornosti

Vodstvo zagotavlja potrebne vire, upravlja tveganja, določa politike, potrjuje rezultate presoj, odloča o izboljšavah in izvaja dolžno nadzorstvo.

Vodja informacijske varnosti izvaja naloge določene s strani vodstva, izvaja nadzorstvo nad izvajanjem politik in ukrepov, koordinira presoje, pripravlja letna poročila in redno poroča vodstvu.

Skrbniki sistemov in lastniki procesov izvajajo in dokumentirajo preverjanja, teste in izboljšave na svojih področjih.

Zaposleni so odgovorni za spoštovanje politik in sodelovanje pri postopkih nadzora ter presojah.

3.7 Veljavnost

Ta politika začne veljati z dnem sprejema vodstva in se uporablja do sprejema nove različice. Organizacija mora hraniti vse različice politike in dokazila o njihovem sprejemu.

Priloge:

- Priloga 1: Matrika ključnih vlog in odgovornosti ZOPS (ang. *RACI*)

[50] CISO ni obvezna vloga po ZInfV-1; velja le za primer, če je CISO imenovan; če ga ni, za te naloge skrbi enota, pristojna za revizijo, notranji nadzor ali druga podobna enota.

Priloga 1: Matrika ključnih vlog in odgovornosti ZOPS (ang. RACI)

Naloga / Aktivnost	Vodstvo organizacije	Vodja informacijske varnosti	Skrbniki sistemov in omrežij	Lastniki informacijskih sredstev	Zaposleni in pogodbeni izvajalci	Vodje oddelkov	Pooblaščene osebe za stik z dobavitelji	Skladnost, DPO, Pravna služba	Notranja revizija
Strateško usmerjanje in odobritev politik varnosti	O, Z	P	S	S	S	S	S	P	P
Zagotavljanje virov za izvajanje varnostnih ukrepov	O, Z	P						P	P
Uvajanje in vzdrževanje politik varnosti	O	Z	S	S	S	S	S	P	P
Svetovanje vodstvu glede varnosti omrežnih in informacijskih sistemov		O, Z						P	P
Usklajevanje odzivov na incidente		O, Z				S	S	P	S
Vzpostavitev in upravljanje varnostnih ukrepov na omrežnih in inf. sistemih	O	Z	Z	Z				P	P
Spremljanje dnevniških zapisov in izvajanje popravkov		S	O, Z						
Opredelitev zahtev glede zaupnosti, razpoložljivosti, celovitosti in avtentičnosti	O	P		Z				P	
Spoštovanje politike varnosti s strani zaposlenih in pogodbenikov	O	P			Z			P	
Poročanje o incidentih - interno	O	S	Z	Z	Z	Z		S	S
Poročanje o incidentih - zunanje	O	Z	P	P	P	P	P	P	P
Izvajanje varnostnih ukrepov na ravni oddelkov	S	P				O, Z		P	P
Ozaveščanje zaposlenih	O	Z				Z			
Varnostna presoja in pogodbeno urejanje z dobavitelji	O	Z					Z	P	
Poročanje in spremljanje skladnosti na področju informacijske varnosti	O	Z						P	P
Izvajanje neodvisnih ocen na področju informacijske varnosti	O								Z

Opombe:

- **Z -** Odgovorna oseba za izvedbo naloge. (Z – Zadolžen); (ang. *R - Responsible*):
- **O -** Oseba, ki je odgovorna za končni izid in odločitve. (O – Odgovoren); (ang. *A - Accountable*):
- **P -** Oseba, s katero je potrebno posvetovati. (P – Posvetovan – se z njim posvetujemo); (ang. *C-Consulted*)
- **S -** Oseba, ki mora biti obveščena o napredku ali odločitvah. (S – Sporočeno – se mu sporoči); (ang. *I - Informed*)