EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PREDSTAVITEV KLJUČNIH KORAKOV ZA VZPOSTAVITEV OKVIRJA POLITIK

Denis ČALETA, ICS-Ljubljana

28 | 01 | 2026

OPREDELITEV TEMELJNIH POJMOV (SUVI)

SUVI - Sistem upravljanja varnosti informacij je **celovit, strukturiran in vnaprej načrtovan sklop politik, postopkov, procesov, odgovornosti in tehničnih ter organizacijskih ukrepov**, s katerimi organizacija **vzpostavlja, izvaja, nadzoruje, vzdržuje in nenehno izboljšuje** varovanje informacij.

Njegov namen je zagotoviti, da so informacije (ne glede na obliko ali medij) **celovite, avtentične, zaupne, in razpoložljive**, ter da je upravljanje tveganj za informacijsko varnost **sistematično, ponovljivo in skladno s standardi** (npr. ISO/IEC 27001) ter zakonskimi zahtevami.

Ključni elementi definicije SUVI vključujejo:
Upravljanje tveganj: prepoznavanje, ocenjevanje in obvladovanje tveganj za informacijsko varnost.
Politike in postopki: jasna pravila, ki vodijo ravnanje zaposlenih in določajo zahteve za varnost.
Organizacijske odgovornosti: določene vloge, pristojnosti in odgovornosti za varovanje informacij.
Ukrepi varnosti: tehnični, fizični in administrativni ukrepi za zaščito informacijskih sredstev.
Nadzor in merjenje: spremljanje učinkovitosti varnostnih ukrepov ter izvajanje notranjih presoj.
Nenehno izboljševanje: redno posodabljanje in izboljševanje sistema na podlagi sprememb tveganj, tehnologije in zakonodaje.

OPREDELITEV TEMELJNIH POJMOV (SUNP)

SUNP – Sistem upravljanja neprekinjenega poslovanja
je organiziran in celovit sistem politik, postopkov in ukrepov, s katerim organizacija zagotavlja, da lahko tudi ob motnjah ali izrednih dogodkih **nadaljuje ključne poslovne procese**, zmanjša vpliv prekinitve ter se čim hitreje povrne v normalno delovanje.

PREGLED KROVNE POLITIKE TER NJENIH PODROČNIH KOMPONENT NA PODROČJU VARNOSTI OMREŽIJ IN INFORMACIJSKIH SISTEMOV

Politika o varnosti omrežnih in informacijskih sistemov (krovna varnostna politika) je strateški dokument, ki določa temeljni pristop organizacije k upravljanju informacijske in kibernetske varnosti ter zaščiti omrežij in informacijskih sistemov.

Zakon **ZInfV-1** zahteva, da imajo vsi zavezanci formalno vzpostavljeno takšno politiko kot del sistema upravljanja varnosti. (ZInfV-1 v 1. točki 22. člena (varnostna dokumentacija) zahteva pripravo politiko ali področne politike o varnosti omrežnih in informacijskih sistemov!)

NAMEN POLITIKE INFORMACIJSKE VARNOSTI

Politika informacijske varnosti 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.

Krovna politika predstavlja **osnovo** varnostnega sistema organizacije in določa splošna načela ter odgovornosti. Na njej nato temeljijo **podporne (sektorske) varnostne politike**, ki urejajo posamezna operativna področja varnosti.

OBSEG POLITIKE

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.

POSEBNA POZORNOST

Politika mora biti 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.

TIPIČNA STRUKTURA POLITIKE

Namen in področje uporabe – kaj in koga politika zavezuje

- ✓ **Pravna in normativna skladnost** – ZInfV-1, GDPR, ISO/IEC 27001 itd.
- ✓ **Varnostni cilji** – celovitost, avtentičnost, zaupnost in razpoložljivost informacij
- ✓ **Upravljavski okvir** – struktura odgovornosti in poročanja
- ✓ **Načela upravljanja tveganj** (ISO 31000 ali NIST)
- ✓ **Načela zaščite informacijskih sistemov**
- ✓ **Ukrepi za odzivanje na incidente**
- ✓ **Varnost dobavne verige**
- ✓ **Izobraževanje in ozaveščanje zaposlenih**
- ✓ **Vzdrževanje in pregled politike**

SEKTORSKE – PODROČNE POLITIKE

Politika informacijske varnosti je lahko razdeljena na več **področnih varnostnih politik**, ki urejajo posamezna področja varnosti:

- Politika ozaveščanja in usposabljanja
- Politika varnosti dobavne verige
- Politika nadzora dostopa
- Politika ravnanja s sredstvi
- Politika varnosti človeških virov
- Politika fizične in okoljske varnost
- Politika upravljanja z ranljivostmi in posodobitvami
- Politika varnostnega kopiranja
- Politika kriptografije
- Politika zaščite pred zlonamerno programsko opremo
- Politika neprekinjenega poslovanja in obvladovanja nesreč
- Politika spremljanja in evidentiranja revizijskih sledi
- Politika uporabe ITK sredstev
- Politika uporabe oblačnih storitev
- Politika uporabe brezžičnih omrežij
- Politika dela od doma in na oddaljenih lokacijah
- Politika čiste mize in zaklepanja zaslona

ODSTOPANJE OD POLITIKE

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.

PRIMER

Primer tabele za odobrena odstopanja (izjeme) od politike informacijske varnosti

ID odstopanja	Opis izjeme	Katero pravilo / zahteva je izvzeto	Razlog izjeme / posebnost	Ocena tveganja	Sprejeti pogoji / kompenzacijski ukrepi	Časovna veljavnost izjeme	Odgovorna oseba	Odobril (funkcija)
EX-001	Uporaba neregistriranega specializiranega sistema	Politika inventarja sredstev	Sistem je kritičen in nezdružljiv z obstoječo opremo	Srednje	Izolacija v ločen VLAN, omejen dostop	1. 1. 2026 – 31. 12. 2026	Vodja proizvodnje	CISO / Vodstvo
EX-002	Oddaljeni dostop brez MFA za specifičnega dobavitelja	Politika dostopa	Dobavitelj ne podpira MFA	Visoko (sprejeto)	Omejitev dostopa po IP, časovno omejeni dostopi	Do nadgradnje sistema	Vodja IT	CISO

VZORČNA DOKUMENTACIJA

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.

RAZLIČEN NIVO IN OBSEG ODGOVORNOSTI TER POOBLASTIL

- Vodstvo organizacije
- Vodja informacijske varnosti (CISO)
- Skrbnik informacijskih sistemov in omrežij
- Lastniki informacijskih sredstev
- Zaposleni in pogodbeni izvajalci
- Vodje organizacijskih enot (oddelkov, sektorjev)
- Pooblaščene osebe za stike z dobavitelji (skrbniki pogodb)
- Kontaktna oseba za informacijsko varnost in njen namestnik

POMOČ PRI POPOLNI IMPLEMENTACIJI ZINFV-1

Standard **ISO/IEC 27001:2022** je tesno usklajen s strukturo **Identify–Protect–Detect–Respond–Recover** okvira CSF in vključuje podobne kontrolne ukrepe kot priloga A standarda **NIST 800-53**.

ZInfV-1 (slovenska implementacija direktive **NIS2**) zahteva od zavezancev vzpostavitev **sistemov upravljanja tveganj in poročanja o incidentih**, ki morajo biti skladni s **funkcionalnim modelom CSF** ter **kontrolnim pristopom 800-53**.

Uporaba kombinacije **CSF + 800-53** omogoča slovenskim **bistvenim** in **pomembnim subjektom**, da izpolnijo **organizacijske zahteve (CSF)** in **tehnične zahteve (800-53)**, kot jih določa direktiva **NIS2** in zakon **ZInfV-1**.

POVEZAVA ISO/IEC 27001 IN SUVI

-**Identifikacija in ocena tveganj**: Organizacije sistematično identificirajo in ocenijo tveganja, povezana z varnostjo informacij. To vključuje dokumentiranje vseh potencialnih groženj in ranljivosti ter oceno njihovega vpliva in verjetnosti.
-**Vzpostavitev varnostnih ukrepov (kontrol)**: Na podlagi ocene tveganj se vzpostavijo ustrezne varnostne kontrole. Te kontrole so dokumentirane in vključujejo tehnične, organizacijske in fizične ukrepe za zaščito informacij.
-**Politike in postopki**: Organizacije razvijejo in dokumentirajo politike in postopke za upravljanje varnosti informacij (politike za dostop do informacij, sredstev, obvladovanje incidentov, varnostno ozaveščanje zaposlenih, ipd.).
-**Nenehno izboljševanje**: Zahteva se nenehno izboljševanje sistema upravljanja varnosti informacij (redni pregledi in posodobitve dokumentacije).
-**Skladnost z zakonodajo**: Dokumentacija mora vključevati vse zakonske in regulativne zahteve, ki veljajo za organizacijo.
-**Notranje in zunanje presoje**: Standard zahteva redne notranje in zunanje presoje, da se preveri skladnost z ISO 27001. Rezultati teh presoj so dokumentirani in uporabljeni za izboljšanje sistema upravljanja varnosti informacij.

STROKOVNI OKVIR NIST CYBER SECURITY FRAMEWORK (CSF)

- **Pet ključnih funkcij**: CSF je razdeljen na pet osnovnih funkcij: identifikacija, zaščita, odkrivanje, odzivanje in obnovitev.
- **Prilagodljivost in skalabilnost**: CSF je zasnovan tako, da je prilagodljiv in uporaben za organizacije vseh velikosti in sektorjev.
- **Profiliranje**: Organizacije lahko ustvarijo profile, ki odražajo njihove specifične potrebe in prioritete glede kibernetske varnosti. To omogoča bolj ciljno usmerjeno in učinkovito upravljanje varnosti.
- **Nenehno izboljševanje**: CSF spodbuja nenehno izboljševanje kibernetske varnosti z rednim pregledovanjem in posodabljanjem varnostnih ukrepov ter praks.
- **Sodelovanje in komunikacija**: CSF zagotavlja skupen jezik in strukturo, ki olajšata sodelovanje in komunikacijo med različnimi deležniki znotraj in zunaj organizacije.

NIST 800-53 JE TEHNIČNI IN KONTROLNI KATALOG VARNOSTNIH UKREPOV

Namenjen je zaščiti informacijskih sistemov. Vsebuje **konkretne varnostne kontrole**, razdeljene v domene, ki določajo, **kako izvajati zaščitne ukrepe v praksi**.

✓ **Primer domen kontrol:** NIST 800-53 je idealen za:

- ✓ tehnično implementacijo varnosti
- ✓ dokazovanje skladnosti
- ✓ gradnjo SUVI (Information Security Management System)

Domena	Primeri kontrol
AC – Access Control	Upravljanje pravic in dostopa
AU – Audit & Accountability	Revizijske sledi in nadzor
CM – Configuration Management	Upravljanje konfiguracij
IR – Incident Response	Procesi za odzivanje na incidente
CP – Contingency Planning	Načrti za neprekinjeno poslovanje
SC – System & Communications Protection	Šifriranje, segmentacija omrežij
SI – System Integrity	Antimalware, nadzor nad ranljivostmi

RAZLIKA IN POVEZAVA MED NICT CSF : NIST 800-53

Vidik	NIST CSF	NIST 800-53
Namen	Strateško upravljanje tveganj	Tehnična implementacija
Uporabniki	Vodstvo, varnostni managerji	IT, SOC, sistemski administratorji
Fokus	Kaj narediti	Kako narediti
Uporaba	Okvir zrelosti	Knjižnica kontrol
Razmerje	Strateški nivo	Podroben operativen nivo

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HVALA ZA POZORNOST

Agamemnonos 14, Chalandri 15231
Attiki, Greece

osu-ms-support@enisa.europa.eu

www.enisa.europa.eu