					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P12					Naslov dokumenta: **Politika upravljanja sredstev**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

1. Namen

1.1 Ta politika določa obvezne organizacijske zahteve za identifikacijo, razvrščanje, upravljanje in varovanje informacijskih sredstev v celotnem njihovem življenjskem ciklu. Podpira upravljanje strojne opreme, programske opreme, podatkov, storitev v oblaku in neopredmetenih informacijskih sredstev na ravni celotne organizacije, vključno z mobilnimi, oddaljenimi in s strani tretjih oseb upravljanimi okolji.

1.2 Namen te politike je zagotoviti popolno vidnost nad okoljem informacijskih sredstev organizacije, s čimer se omogočajo učinkovite kontrole informacijske varnosti, dodelitev lastništva, skladnost z regulativnimi zahtevami ter odgovorna izločitev iz uporabe ali odstranitev.

1.3 Politika je usklajena s kontrolo A.5.9 standarda ISO/IEC 27001:2022, saj zahteva vzdrževanje centraliziranega popisa informacij in z njimi povezanih sredstev. Odgovornost zagotavlja tako, da je vsako sredstvo dodeljeno lastniku, zaščita pa se določi na podlagi razvrstitve, poslovne občutljivosti in regulativnih zahtev.

2. Obseg

2.1 Ta politika velja za vse zaposlene, pogodbene izvajalce, zunanje dobavitelje in ponudnike storitev, ki upravljajo informacijska sredstva v lasti organizacije ali pod njenim nadzorom, jih uporabljajo, do njih dostopajo, jih hranijo ali obdelujejo.

2.2 Obseg vključuje vse kategorije sredstev, kot so:

2.2.1 Fizična sredstva: prenosni računalniki, namizni računalniki, mobilne naprave, izmenljivi mediji, tiskalniki, omrežna oprema

2.2.2 Digitalna sredstva: programska oprema, aplikacije, sistemske slike, podatkovne zbirke, podatki iz varnostnih kopij, šifrirni ključi

2.2.3 Informacijska sredstva: strukturirani in nestrukturirani podatki, poročila, elektronska pošta, intelektualna lastnina

2.2.4 Sredstva v oblaku in virtualna sredstva: okolja IaaS, SaaS in PaaS, virtualni stroji, vsebniki

2.2.5 Logična sredstva: domenska imena, licence, uporabniški računi, referenčne konfiguracije

2.3 Politika ureja tudi sredstva, ki se uporabljajo pri delu na daljavo, v hibridnem načinu dela ali v zunanje izvajanih okoljih, ter zagotavlja njihovo zaščito in vidnost tudi takrat, ko niso fizično nameščena v prostorih organizacije.

3. Cilji

3.1 Vzdrževati popoln, točen in ažuren popis vseh informacijskih sredstev organizacije z opredeljenimi atributi lastništva, razvrstitve in lokacije.

3.2 Dodeliti lastnike sredstev, odgovorne za razvrščanje, ravnanje in zaščito sredstev pod njihovim nadzorom, v skladu s politikami upravljanja podatkov in informacijske varnosti.

3.3 Uporabiti ustrezno razvrstitev in označevanje za vsa sredstva na podlagi občutljivosti, kritičnosti in regulativnih zahtev.

3.4 Varovati sredstva glede na njihovo razvrstitev in povezano izpostavljenost tveganjem, vključno s hrambo, dostopom, prenosom in odstranjevanjem.

3.5 Uveljaviti postopke vračila sredstev in varnega odstranjevanja v okviru postopka prenehanja delovnega razmerja, prekinitve pogodbe ali zaključka življenjskega cikla sredstva.

3.6 Podpirati skladnost z okviri, kot so ISO/IEC 27001, GDPR, NIS2, DORA in COBIT 2019, z uporabo strukturiranega upravljanja sredstev in revizijske sledljivosti.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri Politiko upravljanja sredstev in zagotovi dodelitev virov za njeno celovito izvajanje.

4.1.2 Nosi končno odgovornost za zagotavljanje, da so organizacijska sredstva zaščitena in upravljana v skladu z regulativnimi in pogodbenimi obveznostmi.

4.2 Vodja informacijske varnosti (CISO)

4.2.1 Je lastnik Politike upravljanja sredstev in zagotavlja njeno vključitev v širši sistem upravljanja informacijske varnosti (ISMS) organizacije.

4.2.2 Pregleduje izjeme in odstopanja od te politike ter zagotavlja strategije obvladovanja na podlagi tveganj.

4.2.3 Nadzira periodične preglede razvrstitve sredstev, celovitosti popisa sredstev in skladnosti upravljanja življenjskega cikla sredstev.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko je treba pregledati najmanj enkrat letno ali ob:

9.1.1 spremembah zakonskih ali regulativnih obveznosti, ki vplivajo na razvrščanje sredstev ali zahteve glede popisa,

9.1.2 uvedbi novih kategorij sredstev ali platform za upravljanje (npr. izvorne platforme CMDB v oblaku),

9.1.3 ugotovitvah notranje revizije ali varnostnih incidentih, povezanih z neustreznim upravljanjem sredstev,

9.1.4 organizacijskem prestrukturiranju, ki vpliva na lastništvo ali kontrole življenjskega cikla.

9.2 Postopek pregleda začne skrbnik IT-sredstev in ga usklajuje z vodjo informacijske varnosti, nabavo, pravno službo in zadevnimi vodji oddelkov.

9.3 Vmesne preglede lahko sprožijo tudi:

9.3.1 prevzem ali odprodaja poslovnih enot,

9.3.2 spremembe dobaviteljev, ki vplivajo na sredstva, upravljana s strani tretjih oseb,

9.3.3 tehnološke osvežitve, ki vključujejo množično izločanje iz uporabe ali dodeljevanje.

9.4 Vse revizije te politike morajo:

9.4.1 biti upravljane z različicami in shranjene v repozitoriju ISMS,

9.4.2 biti odobrene s strani najvišjega vodstva,

9.4.3 vključevati povzetek sprememb in utemeljitev,

9.4.4 biti sporočene vsem zadevnim zainteresiranim stranem, vključno s posodobljenimi postopki ali usposabljanjem za sisteme, kjer je to primerno.

10. Povezane politike in povezave

10.1 Ta politika se uporablja skupaj z naslednjimi povezanimi politikami in podpira njihovo izvajanje:

10.1.1 P4 - Politika nadzora dostopa: zagotavlja, da je vidnost sredstev usklajena s pravicami dostopa in mehanizmi nadzora v sistemih in podatkovnih okoljih.

10.1.2 P7 - Politika uvajanja in prenehanja delovnega razmerja: ureja pravočasno dodelitev in vračilo fizičnih in logičnih sredstev med prehodi zaposlenih.

10.1.3 P13 - Politika razvrščanja in označevanja podatkov: določa obvezna pravila razvrščanja sredstev, ki določajo postopke označevanja, ravnanja in odstranjevanja.

10.1.4 P14 - Politika hrambe in odstranjevanja podatkov: opredeljuje roke hrambe in metode varnega odstranjevanja digitalnih in fizičnih sredstev, ki vsebujejo informacije.

10.1.5 P22 - Politika beleženja in spremljanja: omogoča sledljivost dostopa do sredstev in njihove uporabe z beleženjem v sistemih, vidnostjo končnih točk in analitiko vedenja.

10.1.6 P30 - Politika odzivanja na incidente: podpira hitro zajezitev in preiskavo kršitev, povezanih s sredstvi, kot so izgubljeni prenosni računalniki ali neevidentirani mediji za shranjevanje.

10.2 Te politike tvorijo usklajeno strukturo upravljanja, ki zagotavlja, da se sredstva skozi celoten življenjski cikel upravljajo varno, natančno evidentirajo in ustrezno obravnavajo.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi standardi informacijske varnosti in regulativnimi okviri, ki zahtevajo robustno upravljanje sredstev skozi celoten življenjski cikel.

11.2 ISO/IEC 27001:

11.2.1 Klavzula 8.1 - od organizacij zahteva načrtovanje, izvajanje in obvladovanje procesov, potrebnih za izpolnjevanje zahtev informacijske varnosti, vključno s tistimi za upravljanje življenjskega cikla sredstev.

11.3 ISO/IEC 27002:2022 - Kontrole 5.9 do 5.11

11.3.1 Kontrola 5.9 - Popis informacij in drugih povezanih sredstev: zahteva ažuren in popoln popis vseh sredstev, pomembnih za obdelavo informacij.

11.3.2 Kontrola 5.10 - Sprejemljiva uporaba informacij in drugih povezanih sredstev: podprta s pravili uporabe, lastništvom in postopki vračila.

11.3.3 Kontrola 5.11 - Vračilo sredstev: izvedeno s formalnimi postopki predaje in izločanja iz uporabe.

11.3.4 Te kontrole vzpostavljajo strukturirane zahteve za identifikacijo, označevanje, vzdrževanje in sledenje organizacijskih sredstev skupaj z ustreznimi odgovornostmi lastnikov in skrbnikov skozi celoten življenjski cikel.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Popis komponent sistema: odraža se skozi centralizirano upravljanje sredstev, vidnost v realnem času in povezavo z operativnimi konfiguracijami.

11.4.2 RA-3 - Ocena tveganja: popisi sredstev služijo kot temeljni elementi za modeliranje groženj in ocenjevanje tveganj.

11.4.3 MP-6 - Sanitizacija medijev: uveljavljena prek varnih metod odstranjevanja, določenih v kontrolah življenjskega cikla sredstev in politiki odstranjevanja podatkov.

11.5 Uredba EU GDPR (2016/679):

11.5.1 Člen 30 - Evidence dejavnosti obdelave: od organizacij zahteva dokumentiranje sistemov, naprav in repozitorijev, ki hranijo ali obdelujejo osebne podatke.

11.5.2 Člen 32 - Varnost obdelave: usklajen z ocenjevanjem tveganj na podlagi sredstev in varnostnimi ukrepi, prilagojenimi razvrščenim sredstvom in kritični infrastrukturi.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Člen 21(2)(a, b): zahteva vidnost sredstev in popis kot temelj za analizo tveganj, zaščito in odziv na incidente kibernetske varnosti.

11.6.2 Člen 21(3): poudarja potrebo po strukturiranem upravljanju sredstev kot delu organizacijske varnostne kulture.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Člen 5 - Upravljanje IKT in notranje kontrole: od finančnih subjektov zahteva nadzor nad sredstvi IKT z jasnimi zahtevami glede popisa, lastništva in zaščite.

11.7.2 Člen 9 - Okvir upravljanja IKT-tveganj: določa, da morajo procesi upravljanja sredstev podpirati zmanjševanje groženj, načrtovanje neprekinjenega poslovanja in odpornost storitev.

11.8 COBIT 2019:

11.8.1 BAI09 - Upravljanje sredstev: neposredno usklajeno s strukturirano identifikacijo, razvrščanjem, uporabo in odstranjevanjem sredstev organizacije.

11.8.2 DSS01 - Upravljane operacije: podpira izvajanje kontrol, ki zagotavljajo zaščito sredstev in stalno operativno upravljanje.

11.8.3 MEA03 - Spremljanje, vrednotenje in ocenjevanje skladnosti: zagotavlja redno revidiranje kontrol upravljanja sredstev in njihove učinkovitosti pri doseganju regulativne skladnosti.