					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P12S					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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Zahteve za upravljanje sredstev
ISO/IEC 27002:2022	Kontrola 5	Kontrole za upravljanje sredstev
NIST SP 800-53 Rev.5	CM-8	Popis komponent sistema
EU NIS2	Člen 21(2)(a)	Sledenje sredstvom za zaščito omrežnih in informacijskih sistemov
EU DORA	Člen 5(8)	Zahteve glede popisa IKT-sredstev
COBIT 2019	BAI	Življenjski cikel upravljanja IT-sredstev
EU GDPR	Člen 30	Evidenca dejavnosti obdelave

1. Namen

1.1 Ta politika določa, kako organizacija prepoznava, evidentira, varuje in izloča iz uporabe svoja informacijska sredstva, vključno s fizičnimi in digitalnimi komponentami.

1.2 Namen te politike je zmanjšati operativna in varnostna tveganja z zagotavljanjem preglednosti, odgovornosti in varnega ravnanja z vsemi poslovnimi sredstvi skozi njihov življenjski cikel.

1.3 Zanesljiv popis sredstev podpira skladnost s predpisi, odzivanje na incidente, načrtovanje neprekinjenega poslovanja in obvladovanje tveganj.

1.4 Ta politika podpira tudi certificiranje po standardu ISO/IEC 27001 ter izkazuje skladnost s pravnimi, finančnimi in kibernetskovarnostnimi obveznostmi v okviru predpisov, kot so GDPR, NIS2 in DORA.

1.5 Za mala in srednje velika podjetja (SME) je preprost, vendar sistematičen pristop k upravljanju sredstev bistven za preprečevanje neupravljanih naprav, uhajanja podatkov ali ugotovitev neskladnosti pri reviziji, zlasti kadar organizacija deluje z omejenimi tehničnimi viri.

2. Področje uporabe

2.1 Ta politika velja za vsa sredstva, ki so v lasti organizacije, v najemu ali jih organizacija kako drugače upravlja, vključno s sredstvi, ki se uporabljajo pri:

2.1.1 delu v pisarni

2.1.2 delu na daljavo ali v hibridnih oblikah dela

2.1.3 terenskem delu ali mobilnem poslovanju

2.1.4 uporabi okolij v oblaku in zunanjega izvajanja

2.2 Vrste sredstev, ki jih ta politika zajema, vključujejo med drugim:

2.2.1 strojno opremo: prenosnike, namizne računalnike, monitorje, telefone, tablice, USB-pogone, usmerjevalnike, tiskalnike, medije za varnostno kopiranje

2.2.2 programsko opremo: nameščene aplikacije, storitve SaaS, operacijske sisteme, protivirusna orodja, licence

2.2.3 podatkovna sredstva: repozitorije poslovnih podatkov, preglednice, evidence o strankah, izvorno kodo

2.2.4 digitalne poverilnice in storitve: domenska imena, digitalna potrdila, ključe API, e-poštne račune, prijave v storitve v oblaku

2.2.5 sredstva za dostop: ključe, pametne kartice, obeske za dostop, biometrične žetone

2.3 Vsi zaposleni, pogodbeni izvajalci in ponudniki storitev tretjih oseb, ki ravnajo s sredstvi organizacije, spadajo v področje uporabe te politike.

2.4 Politika ureja tako kratkoročna sredstva (npr. projektne prenosnike) kot dolgoročna sredstva ter tudi skupna sredstva, ki jih uporablja več oseb.

3. Cilji

3.1 Vzpostaviti in vzdrževati popoln in točen popis vseh relevantnih sredstev, ki se redno posodablja.

3.2 Zagotoviti, da ima vsako sredstvo določenega lastnika, odgovornega za njegovo uporabo, hrambo in vračilo.

3.3 Razvrstiti sredstva glede na občutljivost, vpliv na poslovanje ali regulativni pomen, s čimer se omogoči uporaba ustreznih ravni zaščite.

3.4 Določiti jasne postopke za izdajo sredstev, prerazporeditev, vzdrževanje, prijavo izgube in izločitev iz uporabe.

3.5 Zagotoviti varno ravnanje s sredstvi skozi njihov življenjski cikel ter da so informacije, ki jih hranijo, ob odstranitvi ustrezno zaščitene ali varno izbrisane.

3.6 Zmanjšati verjetnost varnostnih incidentov, ki jih povzročijo neevidentirana, nevrnjena ali neustrezno uporabljena sredstva organizacije.

3.7 Podpreti skladnost z veljavno zakonodajo (npr. načelom odgovornosti iz GDPR) in certifikacijskimi standardi na področju kibernetske varnosti.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Je lastnik te politike in je odgovoren za to, da se prakse upravljanja sredstev izvajajo in upoštevajo v celotni organizaciji.

4.1.2 Pregleduje in odobrava posodobitve popisa sredstev ter po potrebi odobri izločitev sredstva iz uporabe ali njegov prenos.

4.1.3 O vsaki pomembni izgubi, kraji ali neustrezni uporabi sredstev mora biti obveščen.

4.2 Vodja IT ali imenovani skrbnik sredstev

4.2.1 Vzdržuje popis sredstev (npr. v preglednici, sistemu za upravljanje zahtevkov ali enostavnem orodju za sledenje sredstvom).

4.2.2 Določa lastništvo sredstev in spremlja spremembe statusa (npr. novo, v uporabi, v popravilu, izločeno iz uporabe).

4.2.3 Preverja, da so vsa izdana sredstva evidentirana in povezana s posameznikom ali organizacijsko enoto.

4.2.4 Zagotavlja, da so oznake razvrstitve dodeljene in upoštevane (npr. interno, zaupno).

4.2.5 Usklajuje prevzem, sanitizacijo in deaktivacijo sredstev v postopku prenehanja sodelovanja ali izločitve iz uporabe.

4.2.6 O vseh nerešenih neskladnostih v zvezi s sredstvi poroča GM.

[... 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 Ta politika se mora pregledati najmanj enkrat letno in vedno, kadar:

9.1.1 se uvedejo nove vrste tehnologije ali sredstev

9.1.2 se spremenijo postopki sledenja sredstvom (npr. uvedba novih orodij ali platform)

9.1.3 nove regulativne obveznosti vplivajo na sledljivost ali odstranjevanje sredstev

9.1.4 incident ali revizija prepoznata vrzel v obstoječih praksah upravljanja sredstev

9.2 V pregled morata biti vključena GM in vodja IT, pregled pa mora zajemati posodobitve postopkov ravnanja s sredstvi, predlogo popisa in usmeritve za razvrščanje.

9.3 Vse posodobitve morajo biti dokumentirane in sporočene zadevnemu osebju. Voditi se mora evidenca sprememb z upravljanjem različic.

10. Povezane politike in povezave

10.1 P2S – Politika vlog in odgovornosti upravljanja: Določa odgovornosti za lastništvo politik in delovanje IT.

10.2 P4S – Politika nadzora dostopa: Povezuje uporabo sredstev (npr. prenosnikov, mobilnih naprav) s pravicami dostopa uporabnikov ter upravljanjem identitet in dostopa.

10.3 P7S – Politika uvajanja in prenehanja sodelovanja: Zagotavlja, da sta izdaja in vračilo sredstev vključena v procese življenjskega cikla osebja.

10.4 P13S – Politika razvrščanja in označevanja podatkov: Določa pravila za presojo, ali mora biti sredstvo razvrščeno kot interno ali zaupno.

10.5 P30S – Politika odzivanja na incidente: Usmerja postopke odzivanja, če dogodek, povezan s sredstvom, povzroči kršitev varnosti ali zasebnosti.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1: Zahteva operativne kontrole za upravljanje sredstev in njihovo zaščito skozi celotno obdobje uporabe.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.9: Podrobneje določa, kako sredstva prepoznati, določiti lastništvo, razvrstiti in varno upravljati.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-8: Zahteva, da organizacije vzpostavijo in vzdržujejo popis komponent sistema, vključno s strojno opremo, programsko opremo in virtualnimi sredstvi.

11.4 EU GDPR

11.4.1 Člen 30: Zahteva dokumentiranje dejavnosti obdelave osebnih podatkov, kar je odvisno od poznavanja, kje so podatki shranjeni in na katerih sredstvih.

11.5 EU NIS2

11.5.1 Člen 21(2)(a): Zahteva tehnične in organizacijske ukrepe, vključno s sledenjem sredstvom, za zaščito omrežnih in informacijskih sistemov.

11.6 EU DORA

11.6.1 Člen 5(8): Finančni subjekti morajo kot del upravljanja tveganj IKT vzdrževati podrobne popise sredstev IKT.

11.7 COBIT 2019

11.7.1 BAI09: Določa, da je treba IT-sredstva upravljati skozi njihov življenjski cikel, od nabave do izločitve iz uporabe, z jasno določenim lastništvom in kontrolami.