					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P12S					Naziv dokumenta: **Politika upravljanja imovinom**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Zahtjevi za upravljanje imovinom
ISO/IEC 27002:2022	Kontrola 5	Kontrole upravljanja imovinom
NIST SP 800-53 Rev.5	CM-8	Popis komponenti sustava
EU NIS2	Članak 21(2)(a)	Praćenje imovine radi zaštite mrežnih i informacijskih sustava
EU DORA	Članak 5(8)	Zahtjevi za popis IKT imovine
COBIT 2019	BAI	Upravljanje životnim ciklusom IT imovine
GDPR EU	Članak 30	Evidencija aktivnosti obrade

1. Svrha

1.1 Ova politika definira kako organizacija identificira, evidentira, štiti i stavlja izvan uporabe svoju informacijsku imovinu, uključujući fizičku i digitalnu imovinu.

1.2 Cilj je smanjiti operativne i sigurnosne rizike održavanjem preglednosti, odgovornosti i sigurnog postupanja sa svom poslovnom imovinom tijekom njezina životnog ciklusa.

1.3 Pouzdan Popis imovine podupire usklađenost s regulatornim zahtjevima, odgovor na incidente, planiranje kontinuiteta poslovanja i upravljanje rizicima.

1.4 Ova politika također podupire certifikaciju prema normi ISO/IEC 27001 i demonstrira usklađenost s pravnim, financijskim i kibernetičko-sigurnosnim obvezama prema okvirima kao što su GDPR, NIS2 i DORA.

1.5 Za mala i srednja poduzeća (SME), jednostavan, ali sustavan pristup upravljanju imovinom ključan je za izbjegavanje neupravljanih uređaja, gubitka podataka ili nalaza u reviziji, osobito kada organizacija raspolaže ograničenim tehničkim resursima.

2. Područje primjene

2.1 Ova se politika primjenjuje na svu imovinu u vlasništvu organizacije, u najmu ili kojom organizacija na drugi način upravlja, uključujući imovinu koja se koristi u:

2.1.1 radu u uredu

2.1.2 radu na daljinu ili u hibridnom radu

2.1.3 terenskom radu ili mobilnim operacijama

2.1.4 okruženjima u oblaku i izdvojenim okruženjima

2.2 Obuhvaćene vrste imovine uključuju, ali nisu ograničene na:

2.2.1 Hardver: prijenosna računala, stolna računala, monitori, telefoni, tableti, USB memorije, usmjernici, pisači, mediji za sigurnosne kopije

2.2.2 Softver: instalirane aplikacije, SaaS usluge, operacijski sustavi, antivirusni softver, licence

2.2.3 Podatkovnu imovinu: repozitorije poslovnih podataka, proračunske tablice, evidencije klijenata, izvorni kod

2.2.4 Digitalne vjerodajnice i usluge: nazive domena, digitalne certifikate, API ključeve, račune e-pošte, korisničke račune u uslugama u oblaku

2.2.5 Sredstva za pristup: ključeve, pametne kartice, privjeske za pristup, biometrijske tokene

2.3 Svi zaposlenici, ugovorni izvođači i pružatelji usluga trećih strana koji rukuju imovinom organizacije obuhvaćeni su ovom politikom.

2.4 Ova politika uređuje i kratkotrajnu imovinu (npr. prijenosna računala za određeni projekt) i dugotrajnu imovinu, kao i dijeljenu imovinu koju koristi više članova osoblja.

3. Ciljevi

3.1 Uspostaviti i održavati potpun i točan Popis imovine za svu relevantnu imovinu te ga kontinuirano ažurirati.

3.2 Osigurati da svaka stavka imovine ima imenovanog vlasnika odgovornog za njezinu uporabu, pohranu i povrat.

3.3 Klasificirati imovinu prema osjetljivosti, utjecaju na poslovanje ili regulatornoj relevantnosti kako bi se omogućile diferencirane razine zaštite.

3.4 Definirati jasne postupke za izdavanje imovine, preraspodjelu, održavanje, prijavu gubitka i stavljanje izvan uporabe.

3.5 Osigurati sigurno postupanje s imovinom tijekom cijelog životnog ciklusa te zaštitu informacija koje ona sadrži, odnosno njihovo sigurno brisanje pri zbrinjavanju.

3.6 Smanjiti vjerojatnost sigurnosnih incidenata uzrokovanih neevidentiranom, nevraćenom ili nepravilno korištenom imovinom organizacije.

3.7 Poduprijeti usklađenost s primjenjivim zakonima (npr. načelom odgovornosti iz GDPR-a) i standardima certifikacije u području kibernetičke sigurnosti.

4. Uloge i odgovornosti

4.1 Glavni direktor (GM)

4.1.1 Vlasnik je ove politike i odgovoran je za osiguravanje da se prakse upravljanja imovinom uspostave i provode u cijeloj organizaciji.

4.1.2 Pregledava i odobrava ažuriranja Popisa imovine te prema potrebi odobrava stavljanje imovine izvan uporabe ili njezin prijenos.

4.1.3 Mora biti obaviješten o svakom značajnom gubitku, krađi ili zlouporabi imovine.

4.2 IT voditelj ili imenovani skrbnik imovine

4.2.1 Održava Popis imovine (npr. u proračunskoj tablici, sustavu za evidentiranje zahtjeva ili jednostavnom alatu za praćenje imovine).

4.2.2 Dodjeljuje vlasništvo nad imovinom i prati promjene statusa (npr. nova, u uporabi, na popravku, stavljena izvan uporabe).

4.2.3 Provjerava da je sva izdana imovina evidentirana i povezana s pojedincem ili poslovnom jedinicom.

4.2.4 Osigurava da se oznake klasifikacije primjenjuju i poštuju (npr. Za internu uporabu, Povjerljivo).

4.2.5 Koordinira povrat, sanitizaciju i deaktivaciju imovine tijekom izlaznog procesa ili stavljanja izvan uporabe.

4.2.6 Prijavljuje GM-u sva neriješena odstupanja u evidenciji imovine.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje i svaki put kada:

9.1.1 se uvode nove vrste tehnologije ili imovine

9.1.2 se mijenjaju postupci praćenja imovine (npr. uvođenje novih alata ili platformi)

9.1.3 nove regulatorne obveze utječu na sljedivost ili zbrinjavanje imovine

9.1.4 incident ili revizija utvrdi nedostatak u postojećim praksama upravljanja imovinom

9.2 U pregledima moraju sudjelovati GM i IT voditelj te oni moraju uključivati ažuriranja postupaka rukovanja imovinom, predložaka popisa i smjernica za klasifikaciju.

9.3 Sva ažuriranja moraju biti dokumentirana i priopćena zahvaćenom osoblju. Mora se voditi zapisnik promjena pod verzijskom kontrolom.

10. Povezane politike i poveznice

10.1 P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje odgovornost za vlasništvo nad politikama i IT operacije.

10.2 P4S – Politika kontrole pristupa: povezuje uporabu imovine (npr. prijenosna računala, mobilni uređaji) s pravima pristupa korisnika i upravljanjem identitetima.

10.3 P7S – Politika uvođenja u posao i prestanka radnog odnosa: osigurava da su izdavanje i povrat imovine ugrađeni u procese životnog ciklusa osoblja.

10.4 P13S – Politika klasifikacije i označavanja podataka: utvrđuje pravila za određivanje treba li imovina biti klasificirana kao Za internu uporabu ili Povjerljivo.

10.5 P30S – Politika odgovora na incidente: usmjerava postupke odgovora ako događaj povezan s imovinom rezultira sigurnosnim incidentom ili povredom privatnosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1: zahtijeva operativne kontrole za upravljanje imovinom i njezinu zaštitu tijekom uporabe.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.9: detaljno uređuje način identifikacije, dodjele vlasništva, klasifikacije i sigurnog upravljanja imovinom.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: zahtijeva da organizacije uspostave i održavaju popis komponenti sustava, uključujući hardver, softver i virtualnu imovinu.

11.4 GDPR EU

11.4.1 Članak 30: zahtijeva dokumentiranje aktivnosti obrade podataka, što ovisi o tome gdje se podaci pohranjuju i na kojoj imovini.

11.5 EU NIS

11.5.1 Članak 21(2)(a): zahtijeva tehničke i organizacijske mjere, uključujući praćenje imovine, radi zaštite mrežnih i informacijskih sustava.

11.6 EU DORA

11.6.1 Članak 5(8): financijski subjekti moraju održavati detaljne popise IKT imovine kao dio upravljanja IKT rizicima.

11.7 COBIT 2019

11.7.1 BAI09: propisuje da se IT imovinom mora upravljati tijekom cijelog njezina životnog ciklusa — od nabave do stavljanja izvan uporabe — uz jasno vlasništvo i odgovarajuće kontrole.