					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P12					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**

1. Svrha

1.1 Ova politika utvrđuje obvezne organizacijske zahtjeve za identifikaciju, klasifikaciju, upravljanje i zaštitu informacijske imovine tijekom cijelog njezina životnog ciklusa. Podupire upravljanje hardverom, softverom, podacima, imovinom u oblaku i nematerijalnom informacijskom imovinom na razini cijele organizacije, uključujući mobilna, udaljena i okruženja kojima upravljaju treće strane.

1.2 Svrha ove politike jest osigurati potpunu vidljivost nad okruženjem informacijske imovine organizacije kako bi se omogućile učinkovite sigurnosne kontrole, dodjela vlasništva, usklađenost te odgovorno stavljanje izvan uporabe ili zbrinjavanje.

1.3 Ova je politika usklađena s kontrolom A.5.9 norme ISO/IEC 27001:2022 time što propisuje održavanje centraliziranog popisa informacija i povezane imovine. Osigurava odgovornost povezivanjem svake imovine s vlasnikom te primjenom zaštite temeljene na klasifikaciji, u skladu s poslovnom osjetljivošću i regulatornim zahtjevima.

2. Područje primjene

2.1 Ova se politika primjenjuje na sve zaposlenike, ugovorne izvođače, dobavljače trećih strana i pružatelje usluga koji upravljaju informacijskom imovinom u vlasništvu organizacije ili pod njezinom kontrolom, koriste je, pristupaju joj, pohranjuju je ili obrađuju.

2.2 Područje primjene obuhvaća sve kategorije imovine, uključujući:

2.2.1 Fizičku imovinu: prijenosna računala, stolna računala, mobilne uređaje, prijenosne medije, pisače i mrežnu opremu

2.2.2 Digitalnu imovinu: softver, aplikacije, sistemske slike, baze podataka, sigurnosne kopije podataka i ključeve za šifriranje

2.2.3 Informacijsku imovinu: strukturirane i nestrukturirane podatke, izvješća, e-poštu i intelektualno vlasništvo

2.2.4 Imovinu u oblaku i virtualnu imovinu: IaaS, SaaS i PaaS okruženja, virtualne strojeve i kontejnere

2.2.5 Logičku imovinu: nazive domena, licence, korisničke račune i referentne konfiguracije

2.3 Ova politika također uređuje imovinu koja se koristi u okruženjima rada na daljinu, hibridnim ili eksternaliziranim okruženjima te osigurava zaštitu i vidljivost i kada se imovina fizički ne nalazi u prostorijama organizacije.

3. Ciljevi

3.1 Održavati potpun, točan i ažuran popis imovine za svu informacijsku imovinu organizacije, s definiranim atributima vlasništva, klasifikacije i lokacije.

3.2 Dodijeliti vlasnike imovine odgovorne za klasifikaciju, rukovanje i zaštitu imovine pod njihovom odgovornošću, u skladu s politikama upravljanja podacima i sigurnosti.

3.3 Primjenjivati odgovarajuću klasifikaciju i označavanje na svu imovinu na temelju osjetljivosti, kritičnosti i regulatornih zahtjeva.

3.4 Štititi imovinu u skladu s njezinom klasifikacijom i povezanom izloženošću riziku, uključujući pohranu, pristup, prijenos i zbrinjavanje.

3.5 Osigurati povrat imovine i sigurno zbrinjavanje tijekom procesa razduživanja zaposlenika, prestanka ugovora ili završetka životnog ciklusa imovine.

3.6 Podržati usklađenost s okvirima kao što su ISO/IEC 27001, GDPR, NIS2, DORA i COBIT 2019 kroz strukturirano upravljanje imovinom i revizijsku sljedivost.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava Politiku upravljanja imovinom i osigurava dodjelu resursa za njezinu potpunu provedbu.

4.1.2 Snosi krajnju odgovornost za zaštitu i upravljanje organizacijskom imovinom u skladu s regulatornim i ugovornim obvezama.

4.2 Glavni direktor za informacijsku sigurnost (CISO)

4.2.1 Vlasnik je Politike upravljanja imovinom i osigurava njezinu integraciju sa širim sustavom upravljanja informacijskom sigurnošću (ISMS) organizacije.

4.2.2 Pregledava iznimke i odstupanja od ove politike te osigurava mjere ublažavanja temeljene na riziku.

4.2.3 Nadzire periodične revizije klasifikacije imovine, cjelovitosti popisa imovine i usklađenosti životnog ciklusa 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 pregledavati najmanje jednom godišnje ili kao odgovor na:

9.1.1 promjene pravnih ili regulatornih obveza koje utječu na klasifikaciju imovine ili zahtjeve za popis imovine

9.1.2 uvođenje novih kategorija imovine ili platformi za upravljanje (npr. cloud-native CMDB)

9.1.3 nalaze unutarnje revizije ili sigurnosne incidente povezane s neodgovarajućim upravljanjem imovinom

9.1.4 organizacijsko restrukturiranje koje utječe na vlasništvo ili kontrole životnog ciklusa

9.2 Postupak pregleda pokreće voditelj upravljanja IT imovinom, a koordinira ga s CISO-om, nabavom, pravnim poslovima i pogođenim voditeljima odjela.

9.3 Izvanredni pregledi mogu se pokrenuti i zbog:

9.3.1 stjecanja ili izdvajanja poslovnih jedinica

9.3.2 promjena dobavljača koje utječu na imovinu kojom upravljaju treće strane

9.3.3 obnove tehnologije koja uključuje masovno stavljanje izvan uporabe ili dodjelu

9.4 Sve izmjene ove politike moraju:

9.4.1 biti pod verzijskom kontrolom i pohranjene u repozitoriju dokumenata ISMS-a

9.4.2 biti odobrene od strane izvršnog rukovodstva

9.4.3 uključivati sažetak promjena i obrazloženje

9.4.4 biti priopćene svim pogođenim dionicima, uključujući ažurirane postupke ili obuku za sustave, gdje je primjenjivo

10. Povezane politike i poveznice

10.1 Ova se politika primjenjuje zajedno sa sljedećim povezanim politikama i podupire njihovu provedbu:

10.1.1 P4 - Politika kontrole pristupa: osigurava da je vidljivost imovine usklađena s pravima pristupa i mehanizmima kontrole u sustavima i podatkovnim okruženjima.

10.1.2 P7 - Politika onboardinga i offboardinga: uređuje pravodobnu dodjelu i povrat fizičke i logičke imovine tijekom promjena statusa osoblja.

10.1.3 P13 - Politika klasifikacije i označavanja podataka: utvrđuje obvezna pravila klasifikacije imovine, koja određuju označavanje, rukovanje i zbrinjavanje.

10.1.4 P14 - Politika zadržavanja i zbrinjavanja podataka: definira rokove i metode sigurnog zbrinjavanja za digitalnu i fizičku imovinu koja sadrži informacije.

10.1.5 P22 - Politika bilježenja i praćenja: omogućuje sljedivost pristupa imovini i njezine uporabe kroz bilježenje na razini sustava, vidljivost krajnjih točaka i analitiku ponašanja.

10.1.6 P30 - Politika odgovora na incidente: podupire brzo ograničavanje i istragu incidenata povezanih s imovinom, kao što su izgubljena prijenosna računala ili neevidentirani mediji za pohranu.

10.2 Ove politike čine koherentnu strukturu upravljanja kojom se osigurava da se imovinom upravlja sigurno, da je točno evidentirana i da se s njom primjereno postupa tijekom cijelog životnog ciklusa.

11. Referentni standardi i okviri

11.1 Ova je politika usklađena s međunarodno priznatim standardima informacijske sigurnosti i regulatornim okvirima koji zahtijevaju pouzdano upravljanje imovinom tijekom cijelog životnog ciklusa.

11.2 ISO/IEC 27001:

11.2.1 Točka 8.1 - Zahtijeva da organizacije planiraju, provode i nadziru procese potrebne za ispunjavanje zahtjeva informacijske sigurnosti, uključujući zahtjeve za upravljanje životnim ciklusom imovine.

11.3 ISO/IEC 27002:2022 - Kontrole 5.9 do 5.

11.3.1 Točka 5.9 - Popis informacija i druge povezane imovine: zahtijeva ažuran i potpun popis sve imovine relevantne za obradu informacija.

11.3.2 Točka 5.10 - Prihvatljiva uporaba informacija i imovine: podržana pravilima uporabe, vlasništvom i postupcima povrata.

11.3.3 Točka 5.11 - Povrat imovine: provodi se kroz formalne postupke primopredaje i stavljanja izvan uporabe.

11.3.4 Ove kontrole uspostavljaju strukturirane zahtjeve za identifikaciju, označavanje, održavanje i praćenje organizacijske imovine, uz pripadajuće odgovornosti vlasnika i skrbnika tijekom cijelog životnog ciklusa.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Popis komponenti sustava: odražava se kroz centralizirano upravljanje imovinom, vidljivost u stvarnom vremenu i povezivanje s operativnim konfiguracijama.

11.4.2 RA-3 - Procjena rizika: popisi imovine služe kao temeljni elementi za modeliranje prijetnji i vrednovanje rizika.

11.4.3 MP-6 - Sanitizacija medija: provodi se putem sigurnih metoda zbrinjavanja definiranih kontrolama životnog ciklusa imovine i Politikom zbrinjavanja podataka.

11.5 GDPR EU (2016/679):

11.5.1 Članak 30 - Evidencija aktivnosti obrade: zahtijeva da organizacije dokumentiraju sustave, uređaje i repozitorije koji pohranjuju ili obrađuju osobne podatke.

11.5.2 Članak 32 - Sigurnost obrade: usklađen je s vrednovanjem rizika temeljenim na imovini i zaštitnim mjerama prilagođenima klasificiranoj imovini i kritičnoj infrastrukturi.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Članak 21(2)(a, b): nalaže vidljivost i popis imovine kao temelj za analizu rizika, zaštitu i odgovor na incidente kibernetičke sigurnosti.

11.6.2 Članak 21(3): dodatno naglašava nužnost strukturiranog upravljanja imovinom kao dijela organizacijske sigurnosne kulture.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Članak 5 - Upravljanje IKT-om i unutarnja kontrola: zahtijeva da financijski subjekti upravljaju IKT imovinom uz jasan popis, vlasništvo i zahtjeve zaštite.

11.7.2 Članak 9 - Okvir za upravljanje rizicima IKT-a: utvrđuje da procesi upravljanja imovinom moraju podupirati ublažavanje prijetnji, planiranje kontinuiteta i otpornost usluga.

11.8 COBIT 2019:

11.8.1 BAI09 - Upravljanje imovinom: izravno je usklađeno sa strukturiranom identifikacijom, klasifikacijom, uporabom i zbrinjavanjem organizacijske imovine.

11.8.2 DSS01 - Upravljane operacije: podupire provedbu kontrola koje osiguravaju zaštitu imovine i kontinuirano operativno upravljanje.

11.8.3 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: osigurava redovitu reviziju kontrola upravljanja imovinom i njihove učinkovitosti u usklađivanju s regulatornim zahtjevima.