					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P14					Naslov dokumenta: **Politika hrambe podatkov in odstranjevanja**							
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	Klavzuli 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontrole 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR	Členi 5(1)(e), 17, 32	
Direktiva NIS2	Člen 21(2)(a-e)	
Uredba DORA	Členi 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Namen

1.1 Namen te politike je opredeliti organizacijske zahteve za hrambo podatkov in varno odstranjevanje v vseh fazah življenjskega cikla informacij.

1.2 Ta politika zagotavlja skladnost z veljavnimi pravnimi, regulativnimi in pogodbenimi obveznostmi ter preprečuje nepotrebno ali tvegano kopičenje podatkov.

1.3 Politika podpira izvajanje standarda ISO/IEC 27001:2022 z vzpostavitvijo nadzora nad obdobji hrambe podatkov in postopki nepovratnega odstranjevanja. Omogoča sledljivo dokumentiranje zapisov, zahteva hrambo, usklajeno z občutljivostjo razvrstitve, ter zagotavlja pripravljenost na revizijo, regulativni nadzor in pravno razkritje.

1.4 Dodatni namen politike je ohranjanje zaupnosti, celovitosti in razpoložljivosti (CIA) podatkov ter hkratno zmanjševanje poslovnih tveganj, operativnih neučinkovitosti in izpostavljenosti kršitvam zasebnosti, ki izhajajo iz neustrezne hrambe ali uničenja podatkov.

2. Področje uporabe

2.1 Ta politika se uporablja za vsa fizična in digitalna informacijska sredstva, ki so v lasti organizacije, jih organizacija obdeluje ali hrani, vključno s tistimi, ki so pod nadzorom tretjih oseb, odvisnih družb ali zunanjih izvajalcev.

2.2 Področje uporabe med drugim vključuje:

2.2.1 dokumente, datoteke in zapise (v digitalni in papirni obliki),

2.2.2 podatkovne zbirke in arhive,

2.2.3 elektronsko pošto in dnevnike neposrednega sporočanja,

2.2.4 varnostne kopije, sistemske dnevnike in revizijske sledi,

2.2.5 izvorno kodo, podatke aplikacij in sredstva, gostovana v oblaku,

2.2.6 izmenljive medije in odpisano strojno opremo, ki vsebuje podatke.

2.3 Politika ureja operativne zapise in regulirane zbirke podatkov (npr. finančne, pravne, kadrovske, vsebine, povezane s strankami, in vsebine, pomembne za presojo), ne glede na lokacijo hrambe ali sistem.

2.4 Uporablja se za vse organizacijske enote ter vse zaposlene, pogodbene izvajalce in dobavitelje, ki sodelujejo pri ustvarjanju, hrambi, upravljanju ali odstranjevanju podatkov.

3. Cilji

3.1 Zagotoviti, da se podatki hranijo le toliko časa, kolikor je to pravno, pogodbeno ali operativno potrebno, ter da se po prenehanju potrebe varno odstranijo.

3.2 Preprečiti prezgodnji, nepooblaščeni ali nenamerni izbris zapisov, potrebnih za tekoče poslovanje, skladnost, sodne postopke ali namene presoje.

3.3 Vzpostaviti in uveljaviti enotne roke hrambe na podlagi razvrstitve informacij, vrste sredstva, veljavnih predpisov in izpostavljenosti tveganjem.

3.4 Varovati zasebnost in zaupnost podatkov med hrambo in ob odstranjevanju, vključno z uresničevanjem pravic posameznikov, na katere se nanašajo osebni podatki (npr. izbris po 17. členu GDPR).

3.5 Zagotoviti, da so vse metode odstranjevanja podatkov nepovratne, ustrezno dokumentirane in skladne s priznanimi standardi, kot je NIST SP 800-88.

3.6 Zmanjšati operativne neučinkovitosti, stroškovne obremenitve in pravno izpostavljenost, ki jih povzroča predolga hramba ali nesledeno kopičenje zastarelih podatkov.

3.7 Podpreti cilje neprekinjenega poslovanja in okrevanja po nesreči z integriranim upravljanjem hrambe varnostnih kopij in zagovorljivimi praksami arhiviranja podatkov.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri to politiko ter zagotovi ustrezno financiranje, vire in vključitev v programe obvladovanja tveganj podjetja in skladnosti.

4.1.2 Nosi splošno odgovornost za pravno in regulativno skladnost, povezano s hrambo podatkov in varnim odstranjevanjem.

4.2 Vodja informacijske varnosti (CISO)

4.2.1 Je lastnik te politike in odgovarja za opredelitev ter pregled upravljanja hrambe in odstranjevanja v skladu z ISMS.

4.2.2 Zagotavlja, da se zahteve glede hrambe in odstranjevanja na podlagi razvrstitve izvajajo v poslovnih enotah in tehničnih sistemih.

4.2.3 Spremlja skladnost s politiko in po potrebi zahteva korektivne ukrepe.

[... 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 mora biti pregledana letno ali kadar je izpolnjen kateri koli od naslednjih pogojev:

9.1.1 spremembe veljavne zakonodaje ali predpisov, ki vplivajo na hrambo podatkov (npr. posodobitve GDPR, davčnih predpisov ali DORA),

9.1.2 spremembe okvira razvrščanja ali poslovnih procesov, ki vplivajo na faze življenjskega cikla podatkov,

9.1.3 uvedba novih informacijskih sistemov, arhivskih platform ali tehnologij za odstranjevanje medijev,

9.1.4 ugotovitve presoje notranje revizije ali regulativna priporočila, ki izpostavljajo vrzeli v praksah hrambe ali odstranjevanja.

9.2 Pregled vodita vodja informacijske varnosti (CISO) in pooblaščena oseba za varstvo podatkov (DPO), ob sodelovanju pravne službe, funkcije skladnosti, IT in poslovnih enot.

9.3 Osrednji načrt hrambe podatkov (MDRS) in register odstranjevanja se pregledata vzporedno, da se zagotovi:

9.3.1 da roki ostanejo pravilni in odražajo operativne, pravne in regulativne potrebe,

9.3.2 da je dokumentacija o odstranjevanju popolna in primerna za revizijo,

9.3.3 da se zapisi o pravnem zadržanju potrdijo in sprostijo, kadar je to ustrezno.

9.4 Vse posodobitve politike morajo:

9.4.1 biti formalno verzionirane in hranjene v repozitoriju dokumentacije ISMS,

9.4.2 vključevati evidenco sprememb in utemeljitev spremembe,

9.4.3 biti odobrene s strani najvišjega vodstva,

9.4.4 biti sporočene zadevnemu osebju skupaj s posodobljenim usposabljanjem ali usmeritvenim gradivom.

9.5 Kadar pride do pomembnih sprememb politike, morajo prizadeti zaposleni v 30 dneh po objavi opraviti ciljno usposabljanje, da se zagotovi nadaljnja skladnost.

9.6 Povezane politike in povezave

10. Povezane politike in povezave

10.1.1 P4 - Politika nadzora dostopa: zagotavlja, da do podatkov v obdobju njihove hrambe dostopajo samo pooblaščeni posamezniki ter da se podatki po poteku roka omejijo do odstranitve.

10.1.2 P12 - Politika upravljanja sredstev: opredeljuje, katera sredstva vsebujejo podatke, ki zahtevajo časovno načrtovano odstranjevanje, in spremlja njihov življenjski cikel od pridobitve do uničenja.

10.1.3 P13 - Politika razvrščanja in označevanja podatkov: usmerja odločitve o razvrščanju, ki neposredno vplivajo na trajanje hrambe podatkov in zahtevano metodo odstranjevanja.

10.1.4 P15 - Politika varnostnega kopiranja in obnove: določa roke hrambe in postopke odstranjevanja za medije z varnostnimi kopijami in replicirana podatkovna sredstva.

10.1.5 P18 - Politika kriptografskih kontrol: podpira kriptografski izbris pri odstranjevanju ter zahteva šifriranje med hrambo podatkov do njihovega uničenja.

10.1.6 P30 - Politika odzivanja na incidente: aktivira se v primerih, ko neustrezno odstranjevanje povzroči možno izgubo podatkov, kršitev ali regulativno neskladnost.

10.2 Vsaka povezana politika ima vlogo pri uveljavljanju usklajenega modela upravljanja podatkov na področjih razvrščanja, nadzora življenjskega cikla, dostopa in pripravljenosti na revizijo.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi standardi in regulativnimi okviri, ki opredeljujejo varne, skladne in učinkovite prakse upravljanja življenjskega cikla podatkov.

11.2 ISO/IEC 27001:

11.2.1 Klavzula 6.1.3 - načrt obravnave tveganj: podpira zmanjševanje tveganj, povezanih s predolgo hrambo, kršitvami varnosti podatkov ali neuspehi pri odstranjevanju.

11.2.2 Klavzula 8.1 - operativno načrtovanje in nadzor: vzpostavlja kontrole življenjskega cikla, ki urejajo hrambo, arhiviranje in uničenje.

11.3 ISO/IEC 27002:2022 - Kontrole 5.10, 5.12, 5.30, 5: zagotavljajo praktične smernice o sprejemljivi uporabi podatkov, utemeljitvi hrambe, nadzorovanem brisanju in zagovorljivem upravljanju zapisov v skladu s toleranco do tveganja organizacije.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - hramba revizijskih zapisov: zagotavlja zadostno hrambo revizijskih dnevnikov in dokazil o skladnosti.

11.4.2 MP-6 - sanitizacija medijev: zahteva varne in dokumentirane metode uničenja fizičnih in elektronskih medijev.

11.4.3 SI-12 - ravnanje z informacijami: zahteva ustrezno ravnanje s podatki v skladu s kontrolami hrambe in odstranjevanja.

11.4.4 PL-2 - načrt varnosti in zasebnosti sistema: zahteva dokumentirano ravnanje s podatki v življenjskem ciklu na ravni sistema in določbe o varnem odstranjevanju.

11.5 GDPR (Uredba (EU) 2016/679):

11.5.1 Člen 5(1)(e) - minimizacija podatkov in omejitev hrambe: zahteva, da se podatki ne hranijo dlje, kot je potrebno.

11.5.2 Člen 17 - pravica do izbrisa (»pravica do pozabe«): zahteva takojšen in trajen izbris osebnih podatkov na podlagi veljavne zahteve.

11.5.3 Člen 32 - varnost obdelave: krepi varstvo podatkov med hrambo in zahteva varno uničenje zapisov, ki jim je rok potekel.

11.6 Direktiva NIS2 (Direktiva (EU) 2022/2555):

11.6.1 Člen 21(2)(a-e): zahteva, da subjekti sprejmejo politike in tehnične ukrepe za varno ravnanje s podatki, vključno z omejitvami hrambe in metodami odstranjevanja.

11.7 Uredba DORA (Uredba (EU) 2022/2554):

11.7.1 Člen 5 - upravljanje in nadzor: zahteva strukturirano upravljanje tveganj IKT, vključno z varnim ravnanjem z informacijami skozi njihov življenjski cikel.

11.7.2 Člen 9 - okvir upravljanja tveganj IKT: zahteva politike za hrambo podatkov, uničenje in pravno/regulativno skladnost digitalnega poslovanja.

11.8 COBIT 2019:

11.8.1 DSS01 - upravljane operacije: podpira spremljanje hrambe in doslednost v podatkovnih sistemih.

11.8.2 DSS05 - upravljane varnostne storitve: zagotavlja zaščito hranjenih in arhiviranih podatkov do njihovega varnega odstranjevanja.

11.8.3 MEA03 - spremljanje, vrednotenje in ocenjevanje skladnosti: omogoča presojo izvajanja rokov hrambe, postopkov brisanja in izpolnjevanja regulativnih zahtev.