					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P14S					Naslov dokumenta: **Politika hrambe podatkov**							
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**

Usklajeno s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzuli 6.1.3, 8	Zajema obravnavo tveganj, operativne kontrole in zahteve glede hrambe
ISO/IEC 27002:2022	Kontrola 5	Smernice za obdobja hrambe in metode varnega uničenja
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Hramba revizijskih zapisov, sanitizacija medijev, omejitve hrambe podatkov in njihovo uveljavljanje
EU NIS2	Člen 21(2)(a)	Zahtevana je politika upravljanja življenjskega cikla, primerna tveganju
EU DORA	Člen 5(1)	Upravljanje tveganj IKT: razpoložljivost in odstranitev podatkov
COBIT 2019	BAI03.04, DSS01	Kontrole življenjskega cikla informacij, varno odstranjevanje
Uredba (EU) GDPR	Člen 5(1)(e), 17	Podatki se ne hranijo dlje, kot je potrebno; pravica do izbrisa

1. Namen

1.1 Namen te politike je določiti zavezujoča pravila za hrambo in varno odstranjevanje informacij v okolju SME. Zagotavlja, da se zapisi hranijo le toliko časa, kot to zahtevajo zakonodaja, pogodbene obveznosti ali poslovne potrebe, nato pa se varno uničijo.

1.2 Namen te politike je zmanjšati informacijska tveganja, obvladovati pravno izpostavljenost in omejiti hrambo odvečnih ali zastarelih podatkov. Prispeva k skladnosti z ISO/IEC 27001 in okviri varstva zasebnosti, kot je GDPR, z omejevanjem nepooblaščene hrambe osebnih ali občutljivih informacij.

1.3 Dobro strukturiran okvir hrambe in odstranjevanja zmanjšuje operativne stroške, izboljšuje delovanje sistemov in povečuje pripravljenost na presojo. Za SME z omejenimi zmogljivostmi IT predstavlja praktičen način za odgovorno upravljanje digitalnih in fizičnih informacijskih sredstev.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zapise, datoteke, dnevnike, komunikacije in zbirke podatkov, ki jih organizacija ustvari, zbere, obdela ali hrani,

2.1.2 vse zaposlene, pogodbene izvajalce in zunanje ponudnike, ki obdelujejo podatke organizacije,

2.1.3 vse oblike podatkov (npr. papirne, elektronske, slikovne, zvočne ali dnevniške) ter vse nosilce za hrambo (npr. lokalni diski, storitve v oblaku, e-poštni strežniki, varnostne kopije).

2.2 Področje uporabe vključuje:

2.2.1 poslovne dokumente (npr. račune, pogodbe, projektna poročila),

2.2.2 operativne zapise (npr. dnevnike, zgodovino dostopa, posnetke varnostnih kopij),

2.2.3 osebne podatke (npr. kadrovske mape, komunikacijo s strankami, evidence podpore),

2.2.4 podatke, gostovane interno, zunanje ali v hibridnih sistemih,

2.2.5 arhivirane podatke in varnostne kopije, ne glede na to, ali so aktivni ali mirujoči.

2.3 Področje uporabe zajema vse faze življenjskega cikla podatkov, od nastanka do odobrenega odstranjevanja.

3. Cilji

3.1 Določiti enotna pravila hrambe na podlagi pravnih, operativnih in regulativnih meril.

3.2 Preprečiti prezgodnji izbris ključnih zapisov in odpraviti nepotrebno kopičenje podatkov.

3.3 Zagotoviti varno in nepovratno odstranjevanje podatkov, ko hramba ni več potrebna.

3.4 Dodeliti odgovornost za izvajanje odločitev o hrambi in izbrisu ob kadrovskih omejitvah, značilnih za SME.

3.5 Zagotoviti revizijsko sledljivo dokumentacijo za izkazovanje skrbnega ravnanja v skladu z ISO 27001, GDPR, NIS2 in drugimi okviri.

3.6 Spodbujati varno upravljanje življenjskega cikla podatkov brez nepotrebnega tehničnega bremena za osebje brez specializiranega znanja.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Odobri to politiko in nosi odgovornost zanjo.

4.1.2 Zagotovi, da se postopki hrambe in odstranjevanja izvajajo skladno s pravnimi in poslovnimi tveganji.

4.1.3 Po potrebi odobri izjeme, pravno zadržanje in odlog izbrisa.

4.1.4 Začne pregled politike in odobri posodobitve na podlagi poslovnih ali regulativnih sprememb.

4.2 Imenovani lastnik podatkov

4.2.1 Imenuje se za posamezno kategorijo podatkov (npr. finančni podatki, kadrovski podatki, evidence strank).

4.2.2 Razvršča zapise in določa ustrezno obdobje hrambe na podlagi politike in pravnih usmeritev.

4.2.3 Odobri izbris, ko so zahteve glede hrambe izpolnjene.

4.2.4 Podpira notranje presoje z zagotavljanjem konteksta glede logike hrambe in dogodkov odstranjevanja.

[... 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 veljavne zakonodaje (npr. varstvo podatkov, finančno poročanje),

9.1.2 uvedbi novih sistemov ali procesov, ki vplivajo na življenjski cikel podatkov,

9.1.3 ugotovitvah presoje ali incidentih, ki razkrijejo vrzeli v praksah hrambe.

9.2 Pregledi morajo zagotoviti, da evidenca hrambe ostaja popolna in odraža vse glavne kategorije zapisov.

9.3 Posodobitve politike mora odobriti generalni direktor, o njih pa je treba obvestiti zadevno osebje. Najnovejša različica mora biti dostopna in upravljana z različicami.

10. Povezane politike in povezave

10.1 P2S – Politika vlog in odgovornosti upravljanja: določa lastništvo politike in pooblastila za izjeme.

10.2 P13S – Politika razvrščanja in označevanja podatkov: določa, kako se pravila hrambe uskladijo z razvrstitvijo podatkov.

10.3 P12S – Politika upravljanja sredstev: ureja nosilce za hrambo, ki vsebujejo podatke, za katere veljajo zahteve glede hrambe in odstranjevanja.

10.4 P17S – Politika varstva podatkov in zasebnosti: zagotavlja minimizacijo podatkov in podpira zakonito obdelavo v skladu z GDPR.

10.5 P30S – Politika odzivanja na incidente: aktivira se, ko napake pri odstranjevanju ali hrambi povzročijo možno izpostavljenost podatkov.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1.3: zahteva obravnavo tveganj, povezanih z informacijami, vključno s tveganji hrambe.

11.1.2 Klavzula 8.1: določa operativne kontrole življenjskega cikla.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.33: smernice za določanje obdobij hrambe in metod varnega uničenja.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: zahteva hrambo revizijskih zapisov.

11.3.2 MP-6: določa postopke sanitizacije medijev.

11.3.3 SI-12: obravnava omejitve hrambe podatkov in njihovo uveljavljanje.

11.4 Uredba (EU) GDPR

11.4.1 Člen 5(1)(e): podatki se ne smejo hraniti dlje, kot je potrebno.

11.4.2 Člen 17: pravica do izbrisa se uporablja, kadar podatki niso več zakonito hranjeni.

11.5 EU NIS2

11.5.1 Člen 21(2)(a): zahteva organizacijske politike, primerne tveganju, vključno z upravljanjem življenjskega cikla.

11.6 EU DORA

11.6.1 Člen 5(1): upravljanje tveganj IKT vključuje razpoložljivost in odstranjevanje podatkov.

11.7 COBIT 2019

11.7.1 BAI03.04: zahtevane so kontrole življenjskega cikla informacij.

11.7.2 DSS01.06: postopki varnega odstranjevanja kot del varovanja informacijskih sredstev.