					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P14S					Dokumenta nosaukums: **Datu glabāšanas un likvidēšanas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamajiem standartiem un normatīvajiem aktiem

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1.3. punkts, 8. punkts	Ietver riska apstrādi, darbības kontroles pasākumus un glabāšanas prasības
ISO/IEC 27002:2022	5. kontrole	Vadlīnijas glabāšanas termiņu noteikšanai un drošām iznīcināšanas metodēm
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Audita ierakstu glabāšana, datu nesēju sanitizācija, datu glabāšanas ierobežojumi un to piemērošana
ES NIS2	21. panta 2. punkta a) apakšpunkts	Nepieciešama riskam atbilstoša dzīves cikla pārvaldības politika
ES DORA	5. panta 1. punkts	IKT risku pārvaldība: datu pieejamība un dzēšana
COBIT 2019	BAI03.04, DSS01	Informācijas dzīves cikla kontroles pasākumi, droša likvidēšana
ES GDPR	5. panta 1. punkta e) apakšpunkts, 17. pants	Datus nedrīkst glabāt ilgāk, nekā nepieciešams; tiesības uz dzēšanu

1. Mērķis

1.1 Šīs politikas mērķis ir noteikt saistošas prasības informācijas glabāšanai un drošai likvidēšanai MVU vidē. Tā nodrošina, ka ieraksti tiek glabāti tikai tik ilgi, cik to prasa tiesību akti, līgumsaistības vai darbības vajadzības, un pēc tam tiek droši iznīcināti.

1.2 Šīs politikas mērķis ir samazināt informācijas riskus, pārvaldīt tiesisko pakļautību un ierobežot lieku vai novecojušu datu glabāšanu. Tā palīdz nodrošināt atbilstību ISO/IEC 27001 un privātuma regulējumam, piemēram, GDPR, samazinot personas datu vai sensitīvu datu neatļautu glabāšanu.

1.3 Labi strukturēts glabāšanas un likvidēšanas ietvars samazina darbības izmaksas, uzlabo sistēmu veiktspēju un palielina gatavību auditam. MVU ar ierobežotu IT kapacitāti tas nodrošina praktisku pieeju digitālo un fizisko informācijas aktīvu atbildīgai pārvaldībai.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem ierakstiem, datnēm, žurnāliem, saziņas materiāliem un datu kopām, ko organizācija izveido, vāc, apstrādā vai glabā;

2.1.2 visiem darbiniekiem, līgumdarbiniekiem un ārpakalpojumu sniedzējiem, kuri apstrādā organizācijas datus;

2.1.3 visiem datu formātiem (piemēram, papīra, elektroniskam, attēlu, audio vai žurnālu formātam) un visiem glabāšanas nesējiem (piemēram, vietējiem diskiem, mākoņpakalpojumiem, e-pasta serveriem, rezerves kopijām).

2.2 Piemērošanas joma ietver:

2.2.1 biznesa dokumentus (piemēram, rēķinus, līgumus, projektu pārskatus);

2.2.2 darbības ierakstus (piemēram, žurnālus, piekļuves vēsturi, rezerves kopiju momentuzņēmumus);

2.2.3 personas datus (piemēram, personāla lietas, klientu saziņas materiālus, atbalsta ierakstus);

2.2.4 datus, kas izvietoti iekšējās, ārējās vai hibrīdās sistēmās;

2.2.5 arhivētos datus un rezerves kopiju datus neatkarīgi no tā, vai tie ir aktīvi vai neaktīvi.

2.3 Piemērošanas joma aptver visus datu dzīves cikla posmus — no izveides līdz autorizētai likvidēšanai.

3. Mērķi

3.1 Noteikt vienotas glabāšanas prasības, pamatojoties uz tiesiskajiem, darbības un regulatīvajiem kritērijiem.

3.2 Novērst kritisku ierakstu priekšlaicīgu dzēšanu un nepieļaut nevajadzīgu datu uzkrāšanu.

3.3 Nodrošināt drošu un neatgriezenisku datu likvidēšanu, kad to glabāšana vairs nav nepieciešama.

3.4 Noteikt atbildību par glabāšanas un dzēšanas lēmumu īstenošanu, ņemot vērā MVU personāla resursu ierobežojumus.

3.5 Nodrošināt auditam gatavu dokumentāciju, lai pierādītu pienācīgu rūpību saskaņā ar ISO 27001, GDPR, NIS2 un citiem ietvariem.

3.6 Veicināt drošu datu dzīves cikla pārvaldību, neradot nesamērīgu tehnisko slogu personālam bez specializētām zināšanām.

4. Lomas un pienākumi

4.1 ģenerāldirektors (GM)

4.1.1 apstiprina šo politiku un ir tās īpašnieks;

4.1.2 nodrošina, ka glabāšanas un likvidēšanas procedūras tiek ieviestas atbilstoši tiesiskajiem un biznesa riskiem;

4.1.3 nepieciešamības gadījumā apstiprina izņēmumus un juridisko saglabāšanu;

4.1.4 ierosina politikas pārskatīšanu un apstiprina atjauninājumus, pamatojoties uz uzņēmējdarbības vai normatīvo prasību izmaiņām.

4.2 norīkotais datu īpašnieks

4.2.1 tiek noteikts katrai datu kategorijai (piemēram, finanšu, personāla vai klientu ierakstiem);

4.2.2 klasificē ierakstus un nosaka atbilstošo glabāšanas termiņu saskaņā ar politiku un tiesiskajām prasībām;

4.2.3 apstiprina dzēšanu, kad glabāšanas prasības ir izpildītas;

4.2.4 atbalsta iekšējo auditu, sniedzot skaidrojumu par glabāšanas loģiku un likvidēšanas notikumiem.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā vai, iestājoties kādam no šiem apstākļiem:

9.1.1 izmaiņas piemērojamajos tiesību aktos (piemēram, datu privātuma vai finanšu pārskatu jomā);

9.1.2 tiek ieviestas jaunas sistēmas vai procesi, kas ietekmē datu dzīves ciklu;

9.1.3 audita konstatējumi vai incidenti atklāj trūkumus glabāšanas praksē.

9.2 Pārskatīšanā jānodrošina, ka glabāšanas reģistrs ir pilnīgs un atspoguļo visas galvenās ierakstu kategorijas.

9.3 Politikas atjauninājumus apstiprina GM, un par tiem jāpaziņo skartajam personālam. Jaunākajai versijai jābūt pieejamai un pārvaldītai versiju kontrolē.

10. Saistītās politikas un sasaiste

10.1 P2S – Pārvaldības lomu un atbildības politika: nosaka politikas īpašumtiesības un pilnvaras izņēmumu apstiprināšanai.

10.2 P13S – Datu klasifikācijas un marķēšanas politika: nosaka, kā glabāšanas prasības tiek sasaistītas ar datu klasifikāciju.

10.3 P12S – Aktīvu pārvaldības politika: regulē glabāšanas nesējus, kuros ir dati, uz kuriem attiecas glabāšanas vai likvidēšanas prasības.

10.4 P17S – Datu aizsardzības un privātuma politika: nodrošina datu minimizēšanu un atbalsta likumīgu apstrādi saskaņā ar GDPR.

10.5 P30S – Incidentu reaģēšanas politika: tiek aktivizēta, ja likvidēšanas vai glabāšanas nepilnības rada iespējamu datu pakļautību riskam.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 6.1.3. punkts: nosaka ar informāciju saistīto risku, tostarp glabāšanas risku, apstrādi.

11.1.2 8.1. punkts: nosaka dzīves cikla darbības kontroles pasākumus.

11.2 ISO/IEC 27002

11.2.1 5.33. kontrole: vadlīnijas glabāšanas termiņu noteikšanai un drošām iznīcināšanas metodēm.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: nosaka audita ierakstu glabāšanas prasības.

11.3.2 MP-6: nosaka datu nesēju sanitizācijas procedūras.

11.3.3 SI-12: nosaka datu glabāšanas ierobežojumus un to piemērošanu.

11.4 ES GDPR

11.4.1 5. panta 1. punkta e) apakšpunkts: datus nedrīkst glabāt ilgāk, nekā nepieciešams.

11.4.2 17. pants: tiesības uz dzēšanu ir piemērojamas, ja dati vairs netiek glabāti likumīgi.

11.5 ES NIS

11.5.1 21. panta 2. punkta a) apakšpunkts: nosaka riskam atbilstošas organizatoriskās politikas nepieciešamību, tostarp dzīves cikla pārvaldībā.

11.6 ES DORA

11.6.1 5. panta 1. punkts: IKT risku pārvaldība ietver datu pieejamību un dzēšanu.

11.7 COBIT 2019

11.7.1 BAI03.04: nosaka informācijas dzīves cikla kontroles pasākumu nepieciešamību.

11.7.2 DSS01.06: drošas likvidēšanas procedūras kā daļa no informācijas aktīvu aizsardzības.