					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P14					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 regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 6.1.3, 8.1	
ISO/IEC 27002:2022	Kontroles pasākumi 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
ES Vispārīgā datu aizsardzības regula (GDPR)	Panti 5(1)(e), 17, 32	
ES NIS2 direktīva	Pants 21(2)(a-e)	
ES DORA regula	Panti 5, 9	
COBIT 2019	DSS01, DSS05, MEA03	

1. Mērķis

1.1 Šīs politikas mērķis ir noteikt organizācijas prasības datu glabāšanai un drošai likvidēšanai visos informācijas dzīves cikla posmos. Tā nodrošina atbilstību piemērojamajām tiesiskajām, regulatīvajām un līgumiskajām saistībām un novērš nevajadzīgu vai riskantu datu uzkrāšanu.

1.2 Šī politika atbalsta ISO/IEC 27001:2022 ieviešanu, nodrošinot kontroli pār datu glabāšanas termiņiem un neatgriezeniskas likvidēšanas praksi. Tā nodrošina izsekojamu ierakstu uzturēšanu, glabāšanu atbilstoši klasifikācijas jutīgumam un gatavību auditam, regulatoru pārbaudēm un informācijas atklāšanai tiesvedības vajadzībām.

1.3 Šīs politikas mērķis ir arī uzturēt datu konfidencialitāti, integritāti un pieejamību, vienlaikus mazinot biznesa riskus, darbības neefektivitāti un pakļautību privātuma pārkāpumiem, kas rodas neatbilstošas datu glabāšanas vai iznīcināšanas dēļ.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem fiziskajiem un digitālajiem informācijas aktīviem, kas pieder organizācijai vai ko tā apstrādā vai glabā, tostarp aktīviem, kas atrodas trešo pušu, meitasuzņēmumu vai ārpakalpojumu partneru pārziņā.

2.2 Piemērošanas joma ietver, bet neaprobežojas ar:

2.2.1 dokumentiem, datnēm un ierakstiem (digitālā un papīra formā)

2.2.2 datubāzēm un arhīviem

2.2.3 e-pastiem un tūlītējās ziņapmaiņas žurnāliem

2.2.4 rezerves kopijām, sistēmu žurnāliem un audita pēdām

2.2.5 avotkodu, lietojumprogrammu datiem un mākoņvidē izvietotajiem aktīviem

2.2.6 pārnēsājamiem datu nesējiem un nolietotai aparatūrai, kas satur datus

2.3 Politika reglamentē gan darbības ierakstus, gan regulētas datu kopas (piemēram, finanšu, juridisko, personāla, ar klientiem saistīto un auditam būtisko informāciju) neatkarīgi no glabāšanas vietas vai sistēmas.

2.4 Tā attiecas uz visām organizācijas struktūrvienībām un visiem darbiniekiem, līgumslēdzējiem un piegādātājiem, kas ir iesaistīti datu radīšanā, glabāšanā, pārvaldībā vai likvidēšanā.

3. Mērķi

3.1 Nodrošināt, ka dati tiek glabāti tikai tik ilgi, cik tas ir nepieciešams tiesiskām, līgumiskām vai darbības vajadzībām, un pēc šādas vajadzības beigām tiek droši likvidēti.

3.2 Novērst priekšlaicīgu, neatļautu vai nejaušu to ierakstu dzēšanu, kas nepieciešami notiekošām darbībām, atbilstībai, tiesvedībai vai auditam.

3.3 Izveidot un ieviest vienotus glabāšanas grafikus, kas balstīti uz informācijas klasifikāciju, aktīva veidu, piemērojamiem tiesību aktiem un pakļautību riskam.

3.4 Aizsargāt datu privātumu un konfidencialitāti glabāšanas laikā un likvidēšanas brīdī, tostarp nodrošinot datu subjektu tiesību izpildi (piemēram, dzēšanu saskaņā ar GDPR 17. pantu).

3.5 Nodrošināt, ka visas datu likvidēšanas metodes ir neatgriezeniskas, pienācīgi dokumentētas un atbilst atzītiem standartiem, piemēram, NIST SP 800-88.

3.6 Samazināt darbības neefektivitāti, papildu izmaksas un tiesisko pakļautību, ko rada pārmērīga glabāšana vai neuzraudzīti mantotie dati.

3.7 Atbalstīt darbības nepārtrauktības un atjaunošanas pēc avārijas mērķus, izmantojot integrētu rezerves kopiju glabāšanas pārvaldību un pamatotu datu arhivēšanas praksi.

4. Lomas un pienākumi

4.1 Augstākā vadība

4.1.1 Apstiprina šo politiku un nodrošina atbilstošu finansējumu, resursus un integrāciju organizācijas risku pārvaldībā un atbilstības programmās.

4.1.2 Uzņemas vispārējo pārskatatbildību par tiesisko un regulatīvo atbilstību, kas saistīta ar datu glabāšanu un drošu likvidēšanu.

4.2 Galvenais informācijas drošības vadītājs (CISO)

4.2.1 Ir šīs politikas īpašnieks un atbild par glabāšanas un likvidēšanas pārvaldības prasību noteikšanu un pārskatīšanu saskaņā ar informācijas drošības pārvaldības sistēmu (IDPS).

4.2.2 Nodrošina, ka uz klasifikāciju balstītas glabāšanas un likvidēšanas prasības tiek ieviestas biznesa struktūrvienībās un tehniskajās sistēmās.

4.2.3 Uzrauga politikas ievērošanu un nepieciešamības gadījumā nodrošina koriģējošās darbības.

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

9. Pārskatīšanas un aktualizēšanas prasības

9.1 Šī politika jāpārskata katru gadu vai tad, ja iestājas kāds no turpmāk minētajiem apstākļiem:

9.1.1 izmaiņas piemērojamajos tiesību aktos vai regulējumā, kas ietekmē datu glabāšanu (piemēram, GDPR, nodokļu normatīvā regulējuma vai DORA atjauninājumi)

9.1.2 klasifikācijas ietvara vai biznesa procesu izmaiņas, kas ietekmē datu dzīves cikla posmus

9.1.3 jaunu IT sistēmu, arhivēšanas platformu vai datu nesēju likvidēšanas tehnoloģiju ieviešana

9.1.4 iekšējā audita konstatējumi vai regulatoru ieteikumi, kas norāda uz glabāšanas vai likvidēšanas prakses nepilnībām

9.2 Pārskatīšanu vada Galvenais informācijas drošības vadītājs (CISO) un datu aizsardzības speciālists (DPO), iesaistot Juridisko dienestu, atbilstības funkciju, IT un biznesa struktūrvienības.

9.3 Galvenais datu glabāšanas grafiks (MDRS) un likvidēšanas reģistrs jāpārskata vienlaikus, lai nodrošinātu:

9.3.1 grafiku precizitāti un atbilstību darbības, tiesiskajām un regulatīvajām vajadzībām

9.3.2 likvidēšanas dokumentācijas pilnīgumu un auditējamību

9.3.3 juridiskās saglabāšanas ierakstu pārbaudi un atcelšanu, ja tas ir pamatoti

9.4 Jebkuri politikas atjauninājumi:

9.4.1 formāli jāreģistrē versiju pārvaldībā un jāglabā IDPS dokumentu repozitorijā

9.4.2 jāietver grozījumu vēsture un izmaiņu pamatojums

9.4.3 jāsaņem augstākās vadības apstiprinājums

9.4.4 jāpaziņo attiecīgajam personālam, nodrošinot aktualizētus apmācību vai vadlīniju materiālus

9.5 Ja politikā tiek veikti būtiski grozījumi, ietekmētajiem darbiniekiem 30 dienu laikā no publicēšanas jāiziet mērķēta atkārtota apmācība, lai nodrošinātu nepārtrauktu atbilstību.

9.6 Saistītās politikas un sasaiste

10. Saistītās politikas un sasaiste

10.1.1 P4 - Piekļuves kontroles politika: nodrošina, ka glabāšanas periodā datiem piekļūst tikai autorizētas personas un ka datiem, kuru termiņš ir beidzies, līdz likvidēšanai tiek piemēroti piekļuves ierobežojumi.

10.1.2 P12 - Aktīvu pārvaldības politika: nosaka, kuri aktīvi satur datus, kam nepieciešama plānota likvidēšana, un uzrauga to dzīves ciklu no iegādes līdz iznīcināšanai.

10.1.3 P13 - Datu klasifikācijas un marķēšanas politika: nosaka klasifikācijas lēmumus, kas tieši ietekmē datu glabāšanas ilgumu un nepieciešamo likvidēšanas metodi.

10.1.4 P15 - Rezerves kopiju veidošanas un atjaunošanas politika: nosaka glabāšanas termiņus un likvidēšanas procedūras rezerves kopiju datu nesējiem un replicētiem datu aktīviem.

10.1.5 P18 - Kriptogrāfisko kontroles pasākumu politika: atbalsta kriptogrāfisko dzēšanu likvidēšanas vajadzībām un piemēro šifrēšanu datu glabāšanas laikā līdz to iznīcināšanai.

10.1.6 P30 - Incidentu reaģēšanas politika: tiek aktivizēta gadījumos, kad neatbilstoša likvidēšana rada iespējamu datu zudumu, datu aizsardzības pārkāpumu vai regulatīvu pārkāpumu.

10.2 Katrai saistītajai politikai ir nozīme saskaņota datu pārvaldības modeļa ieviešanā klasifikācijas, dzīves cikla kontroles, piekļuves un gatavības auditam jomās.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar globāli atzītiem standartiem un regulatīvajiem ietvariem, kas nosaka drošu, atbilstošu un efektīvu datu dzīves cikla praksi.

11.2 ISO/IEC 27001:2022:

11.2.1 Punkts 6.1.3 - Risku apstrādes plāns: atbalsta ar pārmērīgu glabāšanu, datu aizsardzības pārkāpumiem vai likvidēšanas kļūmēm saistīto risku mazināšanu.

11.2.2 Punkts 8.1 - Darbības plānošana un kontrole: nosaka dzīves cikla kontroles pasākumus, kas reglamentē glabāšanu, arhivēšanu un iznīcināšanu.

11.3 ISO/IEC 27002:2022 - Kontroles pasākumi 5.10, 5.12, 5.30, 5: sniedz praktiskas vadlīnijas par pieņemamu datu izmantošanu, glabāšanas pamatojumu, kontrolētu dzēšanu un pamatotu ierakstu uzturēšanu atbilstoši organizācijas riska tolerancei.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Audita ierakstu glabāšana: nodrošina pietiekamu audita žurnālu un atbilstības pierādījumu glabāšanu.

11.4.2 MP-6 - Datu nesēju sanitizācija: nosaka drošas un dokumentētas fizisko un elektronisko datu nesēju iznīcināšanas metodes.

11.4.3 SI-12 - Informācijas pārvaldība un glabāšana: nosaka atbilstošu datu pārvaldību saskaņā ar glabāšanas un likvidēšanas kontroles pasākumiem.

11.4.4 PL-2 - Sistēmas drošības un privātuma plāns: pieprasa sistēmas līmeņa dokumentāciju par datu dzīves cikla apstrādi un drošas likvidēšanas noteikumiem.

11.5 ES Vispārīgā datu aizsardzības regula (2016/679):

11.5.1 5. panta 1. punkta e) apakšpunkts - glabāšanas ierobežošana: pieprasa neglabāt datus ilgāk, nekā tas ir nepieciešams.

11.5.2 17. pants - tiesības uz dzēšanu (“tiesības tikt aizmirstam”): pieprasa savlaicīgu un neatgriezenisku personas datu dzēšanu pēc pamatota pieprasījuma.

11.5.3 32. pants - apstrādes drošība: nostiprina datu aizsardzību glabāšanas laikā un nosaka drošu to ierakstu iznīcināšanu, kuru termiņš ir beidzies.

11.6 ES NIS2 direktīva (2022/2555):

11.6.1 21. panta 2. punkta a)-e) apakšpunkti: pieprasa organizācijām ieviest politikas un tehniskos pasākumus drošai datu apstrādei, tostarp glabāšanas ierobežojumiem un likvidēšanas metodēm.

11.7 ES DORA regula (2022/2554):

11.7.1 5. pants - pārvaldība un organizācija: nosaka strukturētu IKT risku pārvaldību, tostarp drošu informācijas dzīves cikla pārvaldību.

11.7.2 9. pants - aizsardzība un novēršana: pieprasa politikas datu glabāšanai, iznīcināšanai un digitālo operāciju tiesiskajai un regulatīvajai atbilstībai.

11.8 COBIT 2019:

11.8.1 DSS01 - Operāciju pārvaldība: atbalsta glabāšanas uzraudzību un konsekvenci dažādās datu sistēmās.

11.8.2 DSS05 - Drošības pakalpojumu pārvaldība: nodrošina glabāto un arhivēto datu aizsardzību līdz drošai likvidēšanai.

11.8.3 MEA03 - Atbilstības uzraudzība, izvērtēšana un novērtēšana: nodrošina glabāšanas noteikumu ieviešanas, dzēšanas procedūru un regulatīvo prasību izpildes auditēšanu.