					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P15S					Dokumenta nosaukums: **Rezerves kopēšanas un atjaunošanas 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**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Rezerves kopēšanas kontroles pasākumi atbilstoši IDPS prasībām
ISO/IEC 27002:2022	Kontroles pasākumi 5.29, 8	Paraugprakse rezerves kopēšanai, integrācija ar darbības nepārtrauktību
NIST SP 800-53 Rev.5	CP-9, MP-6	Rezerves kopiju un datu nesēju aizsardzība
ES NIS2	21. panta 2. punkta c) apakšpunkts	Noturība un nepārtrauktība, izmantojot rezerves kopijas
ES DORA	10. panta 1. punkts	IKT nepārtrauktība — rezerves kopijas finanšu nozares organizācijām
COBIT 2019	BAI04.05, DSS04	Rezerves kopijas jādokumentē un jāpārbauda; procesu kontroles pasākumi
ES GDPR	5. panta 1. punkta f) apakšpunkts, 32. panta 1. punkta c) apakšpunkts	Datu integritāte, pieejamība un savlaicīga atjaunošana

1. Mērķis

1.1 Šī politika nosaka, kā organizācijā tiek veikta un pārvaldīta rezerves kopēšana, lai nodrošinātu darbības nepārtrauktību, aizsardzību pret datu zudumu un savlaicīgu atjaunošanu pēc incidentiem.

1.2 Tā nosaka saistošas prasības sistēmu un datu rezerves kopiju izveidei, glabāšanai un atjaunošanai, īpaši MVU vidē bez sarežģītas IT infrastruktūras.

1.3 Šī politika atbalsta auditgatavību un ISO/IEC 27001 sertifikāciju, nodrošinot, ka būtiskie rezerves kopēšanas kontroles pasākumi ir ieviesti, konsekventi piemēroti un regulāri pārskatīti.

1.4 Organizācijas spēja atjaunot darbību pēc tehniskām kļūmēm, nejaušas dzēšanas vai kiberdrošības incidentiem ir atkarīga no šīs politikas stingras ievērošanas.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām darbībai būtiskajām sistēmām un datiem, tostarp:

2.1.1 finanšu ierakstiem, klientu informāciju un personāla datiem;

2.1.2 galddatoriem, klēpjdatoriem, serveriem un mākoņlietotnēm, ko izmanto saimnieciskajā darbībā;

2.1.3 rezerves kopiju datu nesējiem, piemēram, USB datu nesējiem, ārējām glabātuvēm vai mākoņpakalpojumos glabātām rezerves kopijām.

2.2 Tā attiecas arī uz visām personām, kuras ir atbildīgas par rezerves kopēšanas procesu izpildi vai pārvaldību, tostarp:

2.2.1 izpilddirektoru vai norīkotu atbildīgo personu;

2.2.2 ārējiem IT atbalsta pakalpojumu sniedzējiem vai konsultantiem;

2.2.3 visiem darbiniekiem, kuri ir atbildīgi par datu saglabāšanu apstiprinātās glabāšanas vietās.

3. Mērķi

3.1 Nodrošināt, ka visiem kritiskajiem darbības datiem un sistēmām rezerves kopijas tiek veidotas drošā veidā un atbilstošos intervālos, pamatojoties uz risku un darbības vajadzībām.

3.2 Nodrošināt, ka pēc traucējumiem datus var atjaunot savlaicīgi un pilnā apjomā.

3.3 Novērst neatļautu piekļuvi, manipulācijas vai rezerves kopiju datu zudumu, izmantojot efektīvus glabāšanas kontroles pasākumus.

3.4 Skaidri noteikt un piemērot lomas un pienākumus rezerves kopēšanas procedūru ieviešanai un testēšanai.

3.5 Atbalstīt atbilstību ISO/IEC 27001, GDPR un citām regulatīvajām prasībām, izmantojot strukturētu un dokumentētu rezerves kopēšanas praksi.

4. Lomas un pienākumi

4.1 Izpilddirektors (GM)

4.1.1 apstiprina šo politiku un nodrošina tās ieviešanu;

4.1.2 piešķir resursus un nosaka atbildību par rezerves kopēšanas un atjaunošanas darbībām;

4.1.3 pārskata rezerves kopiju neveiksmes, incidentus vai atkāpes no politikas;

4.1.4 vada politikas ikgadējo pārskatīšanu un nodrošina auditgatavību.

4.2 Ārējs IT atbalsta pakalpojumu sniedzējs (ja piemērojams)

4.2.1 ievieš un pārvalda rezerves kopēšanas risinājumus (lokālus vai mākoņpakalpojumos balstītus);

4.2.2 uzrauga sekmīgu rezerves kopiju izpildi un plāno atjaunošanas testus;

4.2.3 nekavējoties ziņo GM par kļūmēm un incidentiem;

4.2.4 nodrošina šifrēšanu, piekļuves ierobežojumus un pareizu apiešanos ar rezerves kopiju datu nesējiem.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika GM jāpārskata vismaz reizi gadā. Starpposma pārskatīšanu var ierosināt:

9.1.1 būtiskas izmaiņas sistēmās vai glabāšanas metodēs;

9.1.2 jaunu mākoņpakalpojumu vai IT platformu ieviešana;

9.1.3 tiesiskas vai regulatīvas izmaiņas, kas ietekmē datu atjaunošanu;

9.1.4 auditu vai incidentu konstatējumi.

9.2 GM ir atbildīgs par pārskatīšanas uzsākšanu, izmaiņu apstiprināšanu un informēšanu par atjauninājumiem.

9.3 Politikas versijas jāuzskaita un jāarhivē. Aizstātajām versijām jāpiemēro piekļuves ierobežojumi, lai novērstu pārpratumus auditu vai darbības atjaunošanas gadījumos.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir saskaņota ar turpmāk minētajām MVU politikām un ir no tām atkarīga:

10.1.1 P14S – Datu glabāšanas un likvidēšanas politika: nosaka, cik ilgi rezerves kopiju dati jāglabā un kā tie droši jādzēš.

10.1.2 P13S – Datu klasifikācijas un marķēšanas politika: palīdz noteikt prioritātes datiem, kuriem jāveido rezerves kopijas atbilstoši klasifikācijas līmeņiem.

10.1.3 P30S – Incidentu reaģēšanas politika: nosaka procedūras gadījumiem, kad rezerves kopijas neizdodas vai pēc pārkāpuma vai pakalpojuma nepieejamības ir nepieciešama datu atjaunošana.

10.1.4 P2S – Pārvaldības lomu un atbildības politika: nosaka skaidras pilnvaras rezerves kopēšanas pārraudzībai un politikas ieviešanai.

10.1.5 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka personas datu apstrāde rezerves kopijās atbilst tiesiskajām un privātuma prasībām.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8.1. punkts: rezerves kopiju sistēmu operacionālā plānošana un kontrole kā daļa no IDPS.

11.2 ISO/IEC 27002

11.2.1 8.13. kontrole: nosaka paraugpraksi rezerves kopiju plānošanai, uzraudzībai un atjaunošanai.

11.2.2 A pielikuma 5.29. kontrole: nosaka rezerves kopiju integrāciju ar darbības nepārtrauktību un gatavību atjaunošanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (ārkārtas situāciju plānošana): nosaka strukturētas rezerves kopēšanas stratēģijas darbības noturībai.

11.3.2 MP-6 (datu nesēju aizsardzība): paredz drošu apiešanos ar rezerves kopiju datu nesējiem un to iznīcināšanu.

11.4 ES GDPR

11.4.1 5. panta 1. punkta f) apakšpunkts: nosaka personas datu integritāti un pieejamību.

11.4.2 32. panta 1. punkta c) apakšpunkts: nosaka pienākumu savlaicīgi atjaunot piekļuvi personas datiem.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta c) apakšpunkts: paredz rezerves kopijas un atjaunošanu kā daļu no noturības un nepārtrauktības plānošanas.

11.6 ES DORA

11.6.1 10. panta 1. punkts: finanšu nozares organizācijām jānodrošina rezerves kopijas kā daļa no IKT nepārtrauktības pasākumiem.

11.7 COBIT 2019

11.7.1 BAI04.05: paredz dokumentētas rezerves kopēšanas stratēģijas.

11.7.2 DSS04.07: uzsver regulāru testēšanu un kontroli pār datu rezerves kopēšanas un atjaunošanas procesiem.