					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P15					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**

Saskaņots ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1.3., 8. punkts	Risku apstrāde, plānošana un operatīvie rezerves kopēšanas kontroles pasākumi
ISO/IEC 27002:2022	8.13., 5.28., 5.29. kontroles pasākumi	Rezerves kopēšanas pārvaldība, droša likvidēšana un noturība
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Sistēmu rezerves kopēšanas, atjaunošanas un datu nesēju sanitizācijas prasības
ES Vispārīgā datu aizsardzības regula (GDPR)	32. pants, 49. apsvērums	Personas datu atjaunošana un pieejamība, darbības nepārtrauktība
ES NIS2	21. panta 2. punkta c–e apakšpunkts	Rezerves kopēšanas un nepārtrauktības kontroles pasākumi noturībai
ES DORA	10., 11. pants	Finanšu sektora rezerves kopēšanas, atjaunošanas un testēšanas prasības
COBIT 2019	DSS01, DSS04, MEA03	Rezerves kopēšanas operācijas, nepārtrauktība un atbilstības uzraudzība

1. Mērķis

1.1 Šīs politikas mērķis ir noteikt obligātās prasības datu, sistēmu un lietotņu rezerves kopēšanai un atjaunošanai, lai nodrošinātu darbības noturību, datu integritāti un darbības nepārtrauktību.

1.2 Politika nosaka standartizētu ietvaru, lai:

1.2.1 aizsargātu organizācijas datus pret zudumu dzēšanas, bojājuma, atteices vai kiberuzbrukumu dēļ;

1.2.2 noteiktu atjaunošanas prasības, izmantojot skaidri definētus RTO (Recovery Time Objective) un RPO (Recovery Point Objective) parametrus;

1.2.3 integrētu rezerves kopēšanas darbības plašākā ISPD un darbības nepārtrauktības plānu (BCP/DRP) ietvarā;

1.2.4 nodrošinātu atbilstību piemērojamajiem tiesību aktiem un nozares regulējumam attiecībā uz pieejamību un atjaunojamību.

1.3 Politika ievieš ISO/IEC 27001:2022 kontroles pasākumus, kas saistīti ar drošu datu likvidēšanu (5.28), noturību (5.29) un informācijas rezerves kopijām (8.13), un ir saskaņota ar ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA un NIS2 labo praksi.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām darbībai kritiskajām un operatīvajām sistēmām ISPD darbības jomā;

2.1.2 visiem strukturētiem un nestrukturētiem biznesa datiem, tostarp datubāzēm, failiem, e-pastiem un konfigurācijām;

2.1.3 visām vidēm — lokālajai infrastruktūrai, mākoņvidei, hibrīdvidēm un attālinātām glabāšanas vietām ārpus organizācijas telpām;

2.1.4 visam personālam, kas atbild par rezerves kopēšanas procesu pārvaldību, izpildi, pārbaudi vai atjaunošanu.

2.2 Tā attiecas arī uz:

2.2.1 rezerves kopiju datu nesējiem un infrastruktūru, tostarp fiziskajām lentēm, virtuālajām iekārtām, disku momentuzņēmumiem un mākoņpakalpojumos balstītiem rezerves kopēšanas risinājumiem;

2.2.2 trešo pušu pakalpojumu sniedzējiem, ar kuriem noslēgti līgumi par organizācijas rezerves kopiju mitināšanu, pārvaldību vai apstrādi;

2.2.3 žurnālu, konfigurāciju, audita pierakstu un darbības nepārtrauktībai kritiskas operatīvās dokumentācijas rezerves kopijām.

2.3 Sistēmas, kas ir skaidri izslēgtas no rezerves kopēšanas, ir jādokumentē, jāveic to risku izvērtējums, un izslēgšana formāli jāapstiprina ISPD vadītājam un sistēmas īpašniekam.

3. Mērķi

3.1 Nodrošināt, ka visām kritiski svarīgām sistēmām un datiem tiek veidotas uzticamas rezerves kopijas ar pietiekamu biežumu, redundanci un drošības kontroles pasākumiem.

3.2 Nodrošināt atjaunošanas mehānismus, kas atbilst noteiktajām RTO un RPO prasībām saskaņā ar biznesa ietekmes novērtējumiem.

3.3 Uzturēt pilnīgu dokumentāciju par rezerves kopēšanas procedūrām, glabāšanas termiņiem, lomām un izmantotajām tehnoloģijām.

3.4 Validēt rezerves kopēšanas darbību efektivitāti, sistemātiski testējot atjaunošanu, reģistrējot atteices žurnālos un uzraugot trūkumu novēršanas pasākumus.

3.5 Aizsargāt rezerves kopiju datus pret neatļautu piekļuvi, modificēšanu vai iznīcināšanu visā to dzīves ciklā.

3.6 Nodrošināt atbilstību:

3.6.1 ISO/IEC 27001 operatīvo un nepārtrauktības kontroles pasākumu prasībām;

3.6.2 NIST SP 800-53 CP un MP kontroles saimēm rezerves kopēšanas un sanitizācijas jomā;

3.6.3 GDPR 32. pantam un 49. apsvērumam attiecībā uz piekļuves personas datiem atjaunošanu;

3.6.4 DORA 10. pantam un NIS2 21. pantam attiecībā uz IKT nepārtrauktību un noturību.

3.7 Nodrošināt, ka trešo pušu rezerves kopēšanas pakalpojumi atbilst līgumiskajām un regulatīvajām drošības prasībām, tostarp attiecībā uz šifrēšanu, likvidēšanu un paziņošanas protokoliem.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 apstiprina šo politiku un nodrošina, ka darbībai kritiskās sistēmas tiek pienācīgi aizsargātas ar apstiprinātu rezerves kopēšanas un atjaunošanas praksi;

4.1.2 ir atbildīga par to, lai rezerves kopēšanas darbībām tiktu nodrošināti pietiekami resursi un tās periodiski tiktu pārskatītas regulatīvās atbilstības nodrošināšanai.

4.2 Informācijas drošības vadītājs (CISO)

4.2.1 ir šīs politikas īpašnieks un nodrošina tās saskaņotību ar plašākiem informācijas drošības, risku un darbības nepārtrauktības ietvariem;

4.2.2 pārrauga rezerves kopēšanas procedūru integrāciju BCP/DRP, incidentu apstrādē un noturības plānošanā;

4.2.3 pārskata rezerves kopēšanas izņēmumus un izvērtē riska pieņemšanas priekšlikumus attiecībā uz kritisko sistēmu izslēgšanu.

[... 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 agrāk, ja to ierosina:

9.1.1 izmaiņas darbības nepārtrauktības vai avārijas atjaunošanas stratēģijā;

9.1.2 jauni regulatīvie vai tiesiskie pienākumi, kas ietekmē rezerves kopēšanas biežumu vai datu glabāšanu;

9.1.3 izmaiņas sistēmu arhitektūrā, rezerves kopēšanas rīkos vai pakalpojumu sniedzējos;

9.1.4 būtiski incidenti vai audita konstatējumi saistībā ar datu zudumu vai atjaunošanas atteicēm.

9.2 Pārskatīšanu koordinē CISO sadarbībā ar:

9.2.1 IT infrastruktūru un operācijām;

9.2.2 iekšējo auditu;

9.2.3 datu aizsardzības speciālistu;

9.2.4 darbības nepārtrauktības un avārijas atjaunošanas komandām.

9.3 Rezerves kopēšanas grafiki, sistēmu iekļaušanas saraksti, atjaunošanas dokumentācija un izņēmumu žurnāli jāpārskata paralēli, lai nodrošinātu:

9.3.1 precīzu rezerves kopēšanas pārklājumu visiem kritiskajiem aktīviem;

9.3.2 atbilstību RTO/RPO un glabāšanas prasībām;

9.3.3 testēšanas žurnālu un incidentu ziņojumu pilnīgumu;

9.3.4 iepriekš identificēto kontroles trūkumu novēršanu.

9.4 Visiem atjauninājumiem:

9.4.1 jābūt pārvaldītiem ar versiju kontroli un saglabātiem ISPD dokumentu repozitorijā;

9.4.2 jāietver izmaiņu kopsavilkums un pamatojums;

9.4.3 jābūt apstiprinātiem izpildvadībā;

9.4.4 jātiek paziņotiem visam ietekmētajam tehniskajam un biznesa personālam.

10. Saistītās politikas un sasaiste

10.1 Šī politika tieši atbalsta un ir saistīta ar šādiem dokumentiem:

10.1.1 P6 - Risku pārvaldības politika: nosaka uz riskiem balstītu prioritizāciju sistēmu un pakalpojumu rezerves kopiju aizsardzībai.

10.1.2 P12 - Aktīvu pārvaldības politika: nodrošina, ka sistēmas, kurām jāveido rezerves kopijas, ir iekļautas uzskaitē un sasaistītas ar dzīves cikla uzskaiti un klasifikāciju.

10.1.3 P13 - Datu klasifikācijas un marķēšanas politika: nosaka, kurām datu kategorijām nepieciešamas rezerves kopijas, tostarp prioritizēšanai nepieciešamos marķēšanas metadatus.

10.1.4 P14 - Datu glabāšanas un likvidēšanas politika: koordinē rezerves kopiju glabāšanu ar normatīvajiem glabāšanas ierobežojumiem un pareizu datu nesēju likvidēšanu pēc termiņa beigām.

10.1.5 P16 - Datu maskēšanas un pseidonimizācijas politika: atbalsta datu minimizēšanu sensitīvu datu kopu rezerves kopēšanas laikā.

10.1.6 P30 - Incidentu reaģēšanas politika: tiek aktivizēta rezerves kopēšanas atteiču, atjaunošanas problēmu vai rezerves kopiju datu repozitoriju kompromitēšanas gadījumā.

10.2 Šīs savstarpēji saistītās politikas veido vienotu ietvaru, kas nodrošina, ka rezerves kopiju pārvaldība ir integrēta organizācijas plašākajā ISPD un darbības noturības stratēģijā.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 6.1.3. punkts - Risku apstrādes plāns: atbalsta uz riskiem balstītu rezerves kopēšanas prioritizāciju un atjaunošanas plānošanu.

11.1.2 8.1. punkts - Operatīvā plānošana un kontrole: integrē atjaunošanas un nepārtrauktības kontroles pasākumus kā daļu no operatīvajiem drošības pasākumiem.

11.1.3 A pielikuma 5.28. kontrole - Droša iekārtu likvidēšana vai atkārtota izmantošana: attiecas uz drošu rezerves kopiju datu nesēju sanitizāciju.

11.1.4 A pielikuma 5.29. kontrole - Informācijas drošība traucējumu laikā: nodrošina atjaunošanas iespējas incidentu vai katastrofu laikā.

11.1.5 A pielikuma 8.13. kontrole - Informācijas rezerves kopijas: tieši īstenota ar plānotām, testētām un drošām rezerves kopēšanas darbībām.

11.2 ISO/IEC 27002:2022 - 8.13., 5.28., 5.29. kontroles pasākumi: šie kontroles pasākumi nostiprina prasību par regulārām rezerves kopijām, integritātes validāciju un atjaunošanas plānošanu visās IT vidēs.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Sistēmu rezerves kopijas: nosaka visaptverošas rezerves kopēšanas procedūras, tostarp glabāšanu ārpus objekta un atjaunošanas testēšanu.

11.3.2 CP-10 - Sistēmu atjaunošana un restaurācija: pieprasa validētas procedūras pilnīgai vai daļējai atjaunošanai atbilstoši atjaunošanas mērķiem.

11.3.3 MP-6 - Datu nesēju sanitizācija: nodrošina drošu novecojušu rezerves kopiju datu nesēju apstrādi.

11.3.4 SI-12 - Informācijas apstrādes procedūras: nostiprina rezerves kopēšanas un atjaunošanas pienākumus sensitīvu datu aizsardzībai.

11.4 ES Vispārīgā datu aizsardzības regula (GDPR) (2016/679):

11.4.1 32. pants - Apstrādes drošība: nosaka atjaunošanas iespējas un datu pieejamības drošības pasākumus, īpaši personas datiem.

11.4.2 49. apsvērums: atbalsta darbības nepārtrauktības un avārijas atjaunošanas pasākumus, tostarp drošas rezerves kopijas kā daļu no organizācijas noturības.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta c–e apakšpunkts: pieprasa tehniskos un organizatoriskos pasākumus, tostarp rezerves kopēšanas un nepārtrauktības kontroles pasākumus, lai nodrošinātu pakalpojumu noturību.

11.6 ES DORA (2022/2554):

11.6.1 10. pants - IKT darbības nepārtrauktība: pieprasa finanšu iestādēm nodrošināt pilnas datu rezerves kopijas, atjaunošanu un nepārtrauktības plānošanu.

11.6.2 11. pants - IKT darbības nepārtrauktības plānu testēšana: uzsver atjaunošanas spēju validāciju ar regulāru testēšanu.

11.7 COBIT 2019:

11.7.1 DSS01 - Pārvaldītas operācijas: atbalsta uzticamu pakalpojumu sniegšanu, nodrošinot aizsargātu datu pieejamību.

11.7.2 DSS04 - Pārvaldīta nepārtrauktība: nosaka stratēģiskos un operatīvos nepārtrauktības kontroles pasākumus, tostarp verificētas rezerves kopijas.

11.7.3 MEA03 - Uzraudzīt, izvērtēt un novērtēt atbilstību: nosaka periodisku nepārtrauktības pasākumu pārskatīšanu, tostarp rezerves kopēšanas kontroles pasākumu efektivitāti.