					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P32					Dokumenta nosaukums: **Darbības nepārtrauktības un avārijas seku novēršanas 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	8. nodaļa	
ISO/IEC 27002:2022	Kontroles pasākumi 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 līdz CP-11	
NIST SP 800-34 Rev.1	Nepārtrauktības plānošana	Ietvars
ISO 22301:2019		Darbības nepārtrauktības pārvaldības sistēmas prasības
ES GDPR	32. pants	
ES NIS2	21. panta 2. punkta f) apakšpunkts	
ES DORA	10. pants	
COBIT 2019	DSS	

1. Mērķis

1.1. Šī politika nosaka obligātos kontroles pasākumus un pienākumus, lai nodrošinātu organizācijas spēju uzturēt vai atjaunot kritiskās darbības un tās atbalstošos IKT pakalpojumus traucējoša incidenta laikā un pēc tā.

1.2. Tās mērķis ir aizsargāt dzīvību, darbības stabilitāti, tiesisko pienākumu izpildi, saistības pret klientiem un organizācijas reputāciju, stiprinot noturību ar proaktīvu plānošanu un validētām atjaunošanas spējām.

1.3. Šī politika veido pamatu organizācijas darbības nepārtrauktības pārvaldības (BCM) un avārijas seku novēršanas (DR) ietvaram, nodrošinot atbilstību piemērojamajām normatīvajām, līgumiskajām un nozares prasībām.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām organizācijas struktūrvienībām, informācijas sistēmām, darbības procesiem, personālu un trešo pušu pakalpojumiem, kas saskaņā ar biznesa ietekmes analīzes (BIA) rezultātiem ir klasificēti kā kritiski vai būtiski.

2.2. Politika aptver:

2.2.1. dabas un cilvēka izraisītus traucējumus, tostarp kiberuzbrukumus, infrastruktūras atteices, datu centru nepieejamību, pandēmijas un piegādātāju pakalpojumu pārtraukumus

2.2.2. darbības nepārtrauktības plānu (BCP) un avārijas seku novēršanas plānu (DRP) plānošanu, testēšanu un nepārtrauktu pilnveidošanu

2.2.3. lomas un pienākumus ārkārtas reaģēšanā, atjaunošanas koordinēšanā un incidentu eskalācijā

2.3. Šīs politikas prasības ir saistošas visam personālam, kam noteikti nepārtrauktības vai atjaunošanas pienākumi, tostarp IT personālam, procesu īpašniekiem, krīzes vadītājiem un piegādātājiem.

3. Mērķi

3.1. Nodrošināt darbību un pakalpojumu nepārtrauktību, izmantojot iepriekš definētas un pārbaudītas procedūras, līdz minimumam samazinot darbības, reputācijas un tiesisko ietekmi.

3.2. Atjaunot IKT pakalpojumus noteiktajos atjaunošanas laika mērķos (RTO) un atjaunošanas punkta mērķos (RPO), saskaņojot tos ar organizācijas riska tolerances līmeņiem.

3.3. Noteikt atbildību par darbības nepārtrauktības un avārijas seku novēršanas plānošanu, izpildi un pārvaldību visā organizācijā.

3.4. Nodrošināt, ka nepārtrauktības spējas tiek regulāri testētas, uzturētas un pilnveidotas, pamatojoties uz reālistiskiem scenārijiem un audita konstatējumiem.

3.5. Izpildīt atbilstības pienākumus saskaņā ar ISO, NIST, GDPR, DORA un NIS2, apliecinot pienācīgu rūpību darbības noturības un pieejamības jomā.

4. Lomas un pienākumi

4.1. Izpildvadība

4.1.1. Apstiprina Darbības nepārtrauktības un avārijas seku novēršanas politiku un nodrošina tās stratēģisko saskaņotību.

4.1.2. Piešķir budžetu un resursus darbības nepārtrauktības, ārkārtas reaģēšanas un atjaunošanas vingrinājumu nodrošināšanai.

4.2. Darbības nepārtrauktības vadītājs

4.2.1. Atbild par visas organizācijas BCP izstrādi un uzturēšanu, kā arī par nepārtrauktības testēšanas koordinēšanu.

4.2.2. Uztur BIA grafiku, koordinē apmācības un nodrošina, ka dokumentācija atbilst noteiktajiem atbilstības standartiem.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Šī politika reizi gadā jāpārskata Darbības nepārtrauktības vadītājam un CISO, lai nodrošinātu saskaņotību ar:

9.1.1. izmaiņām darbībā, kritiskajās sistēmās vai infrastruktūrā

9.1.2. mācībām, kas gūtas no incidentiem, auditiem, galda vingrinājumiem vai DR testiem

9.1.3. atjauninātiem normatīvajiem vai līgumiskajiem pienākumiem (piemēram, DORA, GDPR, klientu RTO/RPO prasībām)

9.1.4. izmaiņām organizācijas riska apetītē vai nepārtrauktības stratēģijā

9.2. Pārskatīšanā jāiekļauj:

9.2.1. plānu atbilstības un kontaktinformācijas validācija

9.2.2. RTO, RPO un atjaunošanas līmeņu atkārtota izvērtēšana

9.2.3. rezerves kopiju un DR pakalpojumu kapacitātes novērtēšana

9.2.4. atsauksmes no iesaistītajām pusēm, kas īstenoja nesenos atjaunošanas plānus vai testus

9.3. Visi politikas grozījumi:

9.3.1. jāpārvalda ar versiju kontroli, dokumentējot pamatojumu un iesaistīto pušu apstiprinājumu

9.3.2. jāpaziņo galvenajam personālam un komandām, kuru pienākumi ir atjaunināti

9.3.3. jāatspoguļo atjauninātajās apmācībās, informētības materiālos un darbības procedūrās

9.4. Ārkārtas pagaidu atjauninājumi jāizdod, ja ir būtiskas organizatoriskas izmaiņas, tiesisks pienākums vai kritisks konstatējums, kura dēļ spēkā esošie plāni vai politika vairs nav dzīvotspējīgi.

10. Saistītās politikas un sasaiste

10.1. Šī politika tiek piemērota kopā ar šādiem galvenajiem dokumentiem:

10.1.1. P1 – Informācijas drošības politika: nosaka prasību nodrošināt uz risku balstītas un noturīgas darbības visos apstākļos.

10.1.2. P5 – Izmaiņu pārvaldības politika: nodrošina, ka visas ar atjaunošanu saistītās konfigurācijas vai infrastruktūras izmaiņas tiek veiktas saskaņā ar dokumentētām un apstiprinātām darbplūsmām.

10.1.3. P14 – Datu glabāšanas politika un Datu dzēšanas politika: regulē rezerves kopiju datu nesēju un nepārtrauktības darbībās izmantoto atjaunoto datu dzīves ciklu.

10.1.4. P15 – Rezerves kopiju veidošanas un atjaunošanas politika: nosaka kontroles pasākumus rezerves kopiju biežumam, drošībai un atjaunošanas verifikācijai.

10.1.5. P18 – Kriptogrāfisko kontroles pasākumu politika: nodrošina, ka atjaunošanas procesi atbilst šifrēšanas un konfidencialitātes standartiem.

10.1.6. P22 – Žurnālfailu reģistrēšanas un uzraudzības politika: atbalsta nepārtrauktību ietekmējošu notikumu noteikšanu un eskalāciju.

10.1.7. P30 – Incidentu reaģēšanas politika: nosaka ierobežošanas, eskalācijas un pamatcēloņa novēršanas procesus, kas saskaņoti ar darbības nepārtrauktības ierosinātājiem.

10.1.8. P33 – Audita un atbilstības uzraudzības politika: validē darbības nepārtrauktības un atjaunošanas prakšu integritāti un efektivitāti sistēmās un procesos.

11. Atsauces standarti un ietvari

11.1. Šī politika ir saskaņota ar starptautiski atzītiem darbības nepārtrauktības un avārijas seku novēršanas standartiem, atbalstot auditējamību, noturību un tiesisko atbilstību.

11.2. ISO/IEC 27002

11.2.1. A pielikuma 5.29. kontrole – informācijas drošība traucējumu laikā: nosaka prasību uzturēt drošības kontroles pasākumus nelabvēlīgos apstākļos.

11.2.2. A pielikuma 5.30. kontrole – IKT gatavība darbības nepārtrauktībai: nosaka pienākumu sagatavot, testēt un validēt IKT atjaunošanas spējas.

11.3. ISO 22301:2019 – Darbības nepārtrauktības pārvaldības sistēmas

11.3.1. Nodrošina ietvaru BCM prakses izveidei, ieviešanai un uzturēšanai atbilstoši organizācijas mērķiem un riska sliekšņiem.

11.4. NIST SP 800-34 Rev.1 – Nepārtrauktības plānošanas vadlīnijas

11.4.1. Nosaka labo praksi IT sistēmu nepārtrauktības plāniem, tostarp nepārtrauktības stratēģijas izstrādei, ietekmes analīzei un plānu testēšanai.

11.5. ES GDPR (2016/679)

11.5.1. 32. pants – apstrādes drošība: nosaka prasību nodrošināt apstrādes sistēmu noturību un savlaicīgu personas datu pieejamības un piekļuves atjaunošanu pēc incidenta.

11.6. ES NIS2 direktīva (2022/2555)

11.6.1. 21. panta 2. punkta f) apakšpunkts: nosaka darbības nepārtrauktības un krīzes vadības pasākumus tīklu un informācijas sistēmu drošības nodrošināšanai.

11.7. ES DORA (2022/2554)

11.7.1. 10. pants – IKT darbības nepārtrauktība: nosaka prasību finanšu iestādēm izstrādāt un testēt IKT nepārtrauktības plānus, tostarp uz risku balstītus RTO/RPO un pārslēgšanās spējas.

11.8. COBIT 2019

11.8.1. DSS04 – Nepārtrauktības pārvaldība: aptver visus nepārtrauktības plānošanas aspektus, tostarp apdraudējumu identificēšanu, ietekmes analīzi, atjaunošanas stratēģiju un regulāru testēšanu.