					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P32S					Dokumenta nosaukums: **Darbības nepārtrauktības un avārijas 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 piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontroles pasākumi 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
ES GDPR	Panti 32, 33	
ES NIS2	Pants 21(2)(f)	
ES DORA	Pants 10	
COBIT 2019	DSS04	

1. Mērķis

1.1 Šī politika nodrošina, ka organizācija spēj uzturēt darbības procesus un atjaunot būtiskus IT pakalpojumus traucējošu notikumu laikā un pēc tiem, piemēram, elektroapgādes pārtraukumu, kiberuzbrukumu, izspiedējprogrammatūras infekciju vai sistēmu atteices gadījumā.

1.2 Tā nosaka skaidru darbības nepārtrauktības un avārijas atjaunošanas (BC/DR) plānošanas ietvaru, kas pielāgots MVU bez specializētām IT komandām.

1.3 Šī politika palīdz organizācijai izpildīt obligātās prasības saskaņā ar ISO/IEC 27001:2022, GDPR, NIS2, DORA un COBIT 2019, vienlaikus stiprinot darbības noturību un klientu uzticēšanos.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām darbībai kritiskām sistēmām un pakalpojumiem (piemēram, e-pastu, mākoņkrātuvi, rēķinu izrakstīšanas platformām, klientu ierakstiem);

2.1.2 visiem darbiniekiem un ārējiem IT pakalpojumu sniedzējiem, kas atbild par BC/DR gatavību un izpildi;

2.1.3 visu veidu traucējumiem, tostarp kiberdrošības incidentiem, aparatūras atteicēm, elektroapgādes zudumu, plūdiem un biroja nepieejamību.

2.2 Tā aptver:

2.2.1 rezerves kopiju pārvaldību;

2.2.2 darbības nepārtrauktības plānošanu (BCP);

2.2.3 avārijas atjaunošanas darbības;

2.2.4 personāla apmācību un testēšanu;

2.2.5 juridiskās un regulatīvās reaģēšanas procedūras.

3. Mērķi

3.1 Aizsargāt organizācijas spēju nodrošināt pamatpakalpojumus, neraugoties uz neplānotiem traucējumiem.

3.2 Nodrošināt savlaicīgu sistēmu un datu atjaunošanu atbilstoši iepriekš noteiktiem atjaunošanas laika mērķiem (RTO).

3.3 Nodrošināt, ka viss personāls krīzes situācijās spēj ievērot nepārtrauktības procedūras ar minimālu neskaidrību.

3.4 Uzturēt atbilstību datu aizsardzības un darbības noturības normatīvajām prasībām, tostarp GDPR 32. pantam un NIS2 21. pantam.

3.5 Izveidot praktisku un testējamu nepārtrauktības un atjaunošanas stratēģiju, kas ir piemērota MVU.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 ir BC/DR procesa un šīs politikas īpašnieks;

4.1.2 apstiprina darbības nepārtrauktības plānu (BCP);

4.1.3 koordinē reaģēšanu uz incidentiem un iekšējo komunikāciju traucējumu laikā;

4.1.4 veic normatīvajos aktos noteikto ziņošanu, ja tāda ir nepieciešama (piemēram, paziņošanu par GDPR pārkāpumiem).

4.2 Ārējs IT pakalpojumu sniedzējs / sistēmu administrators

4.2.1 uztur un testē rezerves kopijas;

4.2.2 izpilda avārijas atjaunošanas procedūras, kad tās tiek aktivizētas;

4.2.3 dokumentē visas atjaunošanas darbības un sistēmu atjaunošanas notikumus;

4.2.4 nekavējoties ziņo GM par kritiskiem IT incidentiem.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Politikas un plāna ikgadējā pārskatīšana

9.1.1 Ģenerāldirektoram (GM) jānodrošina, ka šī politika un ar to saistītais darbības nepārtrauktības plāns (BCP) tiek formāli pārskatīti vismaz reizi gadā.

9.1.2 Pārskatīšanā jāiekļauj:

9.1.2.1 jaunu vai aktuālu risku izvērtēšana;

9.1.2.2 RTO/RPO atkārtota validācija;

9.1.2.3 piegādātāju un kontaktinformācijas pārbaude;

9.1.2.4 saskaņošana ar izmaiņām IT sistēmās, juridiskajos pienākumos vai darbībā.

9.2 Atjaunināšana pēc ierosinātājiem

9.2.1 Šī politika jāatjaunina arī, reaģējot uz:

9.2.1.1 būtiskiem incidentiem vai traucējumiem, īpaši, ja mērķi nav sasniegti;

9.2.1.2 jauniem juridiskajiem vai regulatīvajiem pienākumiem (piemēram, DORA grozījumiem);

9.2.1.3 izmaiņām kritiskajās sistēmās, mākoņplatformās vai personālā;

9.2.1.4 konstatējumiem no ikgadējiem BCP/DR testiem.

9.3 Izmaiņu kontroles process

9.3.1 Visas izmaiņas jāapstiprina GM.

9.3.2 Jāuztur versiju vēstures žurnāls, ietverot datumu, izmaiņu aprakstu un apstiprinātāju.

9.3.3 Atjauninātā politika atkārtoti jāizplata visam attiecīgajam personālam, tostarp IT pakalpojumu sniedzējam un struktūrvienību vadītājiem.

9.4 Gūto atziņu dokumentēšana

9.4.1 Pēc testiem vai reāliem traucējumiem dokumentētās gūtās atziņas jāizmanto turpmākajos grozījumos.

9.4.2 Šajās pārskatīšanās jāiekļauj arī piegādātāju snieguma izvērtēšana un reaģēšanas atbilstības pārbaudes.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir cieši integrēta ar šādām SME politikām:

10.1.1 P1S – Informācijas drošības politika: nosaka augsta līmeņa drošības mērķus, kurus darbības nepārtrauktības un atjaunošanas praksei jāatbalsta.

10.1.2 P4S – Piekļuves kontroles politika: nodrošina ārkārtas piekļuves tiesību atsaukšanu vai atjaunošanu lietotājiem darbības traucējumu scenārijos.

10.1.3 P6S – Risku pārvaldības politika: veido pamatu ar darbības nepārtrauktību saistīto risku identificēšanai, izvērtēšanai un prioritizēšanai.

10.1.4 P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka darbinieki ir sagatavoti rīcībai traucējumu laikā un izprot BCP.

10.1.5 P15S – Rezerves kopiju veidošanas un atjaunošanas politika: nosaka konkrētas tehniskās procedūras datu pieejamības aizsardzībai un atjaunošanai.

10.1.6 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka darbības nepārtrauktības plānošanā tiek ievērota personas datu aizsardzība un atbilstība GDPR incidentu laikā un pēc tiem.

10.1.7 P22S – Žurnālfiksēšanas un uzraudzības politika: atbalsta tādu notikumu identificēšanu, kas var aktivizēt BC/DR procesus, un nodrošina audita pēdas digitālās kriminālistikas vajadzībām pēc traucējumiem.

10.1.8 P30S – Incidentu reaģēšanas politika: piemērojama tieši pirms atjaunošanas procesa aktivizēšanas kiberdrošības vai operacionālu incidentu gadījumā.

10.1.9 P31S – Pierādījumu vākšanas un digitālās kriminālistikas politika: nodrošina, ka darbības nepārtrauktības scenāriju laikā tiek iegūti digitālās kriminālistikas pierādījumi atbilstības, apdrošināšanas vai izmeklēšanas vajadzībām.

10.2 Šīs politikas kopā veido saskaņotu, auditam gatavu ietvaru noturībai, pārskatatbildībai un kontroles pasākumu nepārtrauktībai visās SME darbībās.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 Punkts 6.1 – nosaka prasību uz risku balstītai plānošanai un apstrādei, tostarp darbības nepārtrauktībai un atjaunošanai.

11.1.2 Punkts 6.3 – uzsver nepārtrauktu pilnveidi pēc traucējumiem.

11.1.3 Punkts 8.1 – nosaka obligātus darbības kontroles pasākumus, tostarp dokumentētus darbības nepārtrauktības pasākumus.

11.2 ISO/IEC 27002:

11.2.1 5.29. kontrole – nosaka prasību izveidot un uzturēt darbības nepārtrauktības kārtību.

11.2.2 5.30. kontrole – nosaka prasību testēt un pārskatīt šo kārtību.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – definē prasības ārkārtas situāciju plānošanai.

11.3.2 CP-4 – nosaka prasību organizācijas personāla apmācībai ārkārtas situāciju plānošanā.

11.3.3 CP-6 – aptver prasības alternatīvai glabāšanas vietai.

11.3.4 CP-7 – nosaka prasības alternatīvai apstrādes vietai.

11.4 ES GDPR:

11.4.1 Pants 32 – nosaka prasību īstenot pasākumus, lai nodrošinātu apstrādes sistēmu un pakalpojumu nepārtrauktu pieejamību un noturību.

11.4.2 Pants 33 – nosaka paziņošanas pienākumus pārkāpumu gadījumos, kad darbības nepārtrauktības traucējums izraisa personas datu kompromitēšanu.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 Pants 21(2)(f) – nosaka prasību pēc darbības nepārtrauktības plānošanas un krīzes pārvaldības spējām kā kiberrisku gatavības nosacījumu.

11.6 ES DORA regula (2022/2554):

11.6.1 Pants 10 – nosaka prasību ieviest digitālās darbības noturības testēšanas un atjaunošanas spējas, īpaši finanšu sektora MVU.

11.7 COBIT 2019:

11.7.1 DSS04 – Darbības nepārtrauktības pārvaldība: sniedz uzņēmuma pārvaldības vadlīnijas darbības noturības uzturēšanai un validēšanai, tostarp attiecībā uz atbildību, testēšanu, piegādātāju integrāciju un pārskatīšanu pēc notikuma.