					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P32					Dokumendi pealkiri: **Talitluspidevuse ja katastroofitaaste poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	
ISO/IEC 27002:2022	Kontrollid 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 kuni CP-11	
NIST SP 800-34 Rev.1	Talitluspidevuse planeerimine	Raamistik
ISO 22301:2019		Talitluspidevuse juhtimissüsteemi nõuded
ELi GDPR	Artikkel 32	
ELi NIS2	Artikkel 21(2)(f)	
ELi DORA	Artikkel 10	
COBIT 2019	DSS	

1. Eesmärk

1.1. Käesolev poliitika sätestab kohustuslikud kontrollid ja vastutused, et tagada organisatsiooni võime jätkata või taastada kriitilised äritegevused ja neid toetavad IKT-teenused talitlushäiret põhjustanud intsidendi ajal ja järel.

1.2. Poliitika eesmärk on kaitsta elu, tegevuse stabiilsust, õiguslikke kohustusi, klientidele antud lubadusi ja organisatsiooni mainet, lõimides vastupidavuse ennetava planeerimise ning valideeritud taastevõime kaudu.

1.3. Käesolev poliitika loob aluse organisatsiooni talitluspidevuse juhtimise (BCM) ja katastroofitaaste (DR) raamistikule ning tagab kohaldatavate regulatiivsete, lepinguliste ja valdkondlike nõuete täitmise.

2. Kohaldamisala

2.1. Käesolev poliitika kohaldub kõigile organisatsiooni üksustele, infosüsteemidele, äriprotsessidele, töötajatele ja kolmandate osapoolte teenustele, mis on ärimõju analüüsi (BIA) tulemuste alusel klassifitseeritud kriitiliseks või oluliseks.

2.2. Poliitika hõlmab järgmist:

2.2.1. Looduslikud ja inimtekkelised häired, sealhulgas küberrünnakud, taristu rikked, andmekeskuse katkestused, pandeemiad ja tarnijate teenusekatkestused

2.2.2. Äritegevuse järjepidevuse plaanide (BCP) ja katastroofitaaste plaanide (DRP) kavandamine, testimine ning pidev täiustamine

2.2.3. Rollid ja vastutused hädaolukorrale reageerimisel, taaste koordineerimisel ja intsidentide eskaleerimisel

2.3. Kõik töötajad, kellel on talitluspidevuse või taastamisega seotud vastutused, sealhulgas IT, äriüksuste omanikud, kriisijuhid ja tarnijad, peavad järgima käesoleva poliitika sätteid.

3. Eesmärgid

3.1. Tagada äritegevuse ja teenuste talitluspidevus eelnevalt määratletud ja testitud protseduuride kaudu, minimeerides tegevusliku, maine- ja õigusliku mõju.

3.2. Taastada IKT-teenused määratletud taasteaja eesmärgi ja taastepunkti eesmärgi piires kooskõlas äritegevuse riskitaluvusega.

3.3. Määrata kogu organisatsioonis selge vastutus talitluspidevuse ja katastroofitaaste kavandamise, rakendamise ning juhtimise eest.

3.4. Tagada, et talitluspidevuse võimekusi testitakse, hallatakse ja täiustatakse regulaarselt realistlike stsenaariumide ja auditileidude alusel.

3.5. Täita ISO, NIST-i, GDPR-i, DORA ja NIS2 nõuetest tulenevad vastavuskohustused ning toetada hoolsuskohustuse täitmist talitluspidevuse ja käideldavuse tagamisel.

4. Rollid ja vastutused

4.1. Tippjuhtkond

4.1.1. Kinnitab talitluspidevuse ja katastroofitaaste poliitika ning tagab selle strateegilise kooskõla.

4.1.2. Eraldab eelarve ja ressursid talitluspidevuse, hädaolukordadele reageerimise ja taasteõppuste toetamiseks.

4.2. Talitluspidevuse juht

4.2.1. Vastutab organisatsiooniüleste äritegevuse järjepidevuse plaanide väljatöötamise, haldamise ja talitluspidevuse testimise koordineerimise eest.

4.2.2. Hoiab ajakohasena ärimõju analüüsi ajakava, korraldab koolitusi ja tagab, et dokumentatsioon vastab vastavusnõuetele.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Käesolev poliitika tuleb talitluspidevuse juhi ja infoturbejuhi poolt läbi vaadata kord aastas, et tagada kooskõla järgmisega:

9.1.1. Muudatused äritegevuses, kriitilistes süsteemides või taristus

9.1.2. Intsidentidest, audititest, lauaõppustest või DR-testidest saadud õppetunnid

9.1.3. Uuendatud regulatiivsed või lepingulised kohustused (nt DORA, GDPR, klientide RTO/RPO nõuded)

9.1.4. Muudatused organisatsiooni riskivalmiduses või talitluspidevuse strateegias

9.2. Läbivaatamine peab hõlmama järgmist:

9.2.1. Plaanide asjakohasuse ja kontaktandmete valideerimine

9.2.2. RTO-de, RPO-de ja taasteastmete ümberhindamine

9.2.3. Varundus- ja katastroofitaaste teenuste mahu ning võimekuse hindamine

9.2.4. Tagasiside sidusrühmadelt, kes rakendasid hiljutisi taasteplaane või osalesid testides

9.3. Kõik poliitikamuudatused peavad olema:

9.3.1. hallatud versioonihalduses koos dokumenteeritud põhjenduse ja sidusrühmade kinnitusega

9.3.2. teatavaks tehtud võtmetöötajatele ja meeskondadele koos ajakohastatud vastutustega

9.3.3. kajastatud ajakohastatud koolitustes, teadlikkusmaterjalides ja tööprotseduurides

9.4. Erakorralised vahepealsed ajakohastused tuleb välja anda juhul, kui oluline organisatsiooniline muudatus, õiguslik kohustus või kriitiline leid muudab kehtivad plaanid või poliitika mittetoimivaks.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika toimib koostoimes järgmiste põhidokumentidega:

10.1.1. P1 – Infoturbepoliitika: sätestab nõude riskipõhisteks ja vastupidavateks tegevusteks kõigis tingimustes.

10.1.2. P5 – Muudatuste haldamise poliitika: tagab, et kõik taastamisega seotud konfiguratsiooni- või taristumuudatused järgivad dokumenteeritud ja heakskiidetud töövooge.

10.1.3. P14 – Andmete säilitamise ja kõrvaldamise poliitika: reguleerib talitluspidevuse tegevustes kasutatavate varunduskandjate ja taastatud andmete elutsüklit.

10.1.4. P15 – Varundamise ja taastamise poliitika: kehtestab kontrollid varundamise sageduse, turvalisuse ja taastamise kontrolli kohta.

10.1.5. P18 – Krüptograafiliste kontrollimeetmete poliitika: tagab, et taastamisprotsessid järgivad krüpteerimise ja konfidentsiaalsuse nõudeid.

10.1.6. P22 – Logimise ja seire poliitika: toetab talitluspidevust mõjutavate sündmuste tuvastamist ja eskaleerimist.

10.1.7. P30 – Intsidentidele reageerimise poliitika: määratleb talitluspidevuse käivitajatega kooskõlas olevad ohjeldamise, eskaleerimise ja algpõhjuse käsitlemise protsessid.

10.1.8. P33 – Auditi ja vastavusseire poliitika: valideerib talitluspidevuse ja taastamise praktikate terviklikkuse ning tõhususe süsteemide ja protsesside lõikes.

11. Viitestandardid ja raamistikud

11.1. Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud talitluspidevuse ja katastroofitaaste standarditega ning toetab auditeeritavust, vastupidavust ja õigusnormidele vastavust.

11.2. ISO/IEC 27002

11.2.1. Lisa A kontroll 5.29 – infoturve häirete ajal: nõuab turbekontrollide toimepidevust ebasoodsates tingimustes.

11.2.2. Lisa A kontroll 5.30 – IKT valmisolek talitluspidevuseks: nõuab IKT taastevõimekuste ettevalmistamist, testimist ja valideerimist.

11.3. ISO 22301:2019 – talitluspidevuse juhtimissüsteemid

11.3.1. Annab raamistiku talitluspidevuse praktikate kehtestamiseks, rakendamiseks ja haldamiseks kooskõlas organisatsiooni eesmärkide ja riskitaluvusega.

11.4. NIST SP 800-34 Rev.1 – talitluspidevuse planeerimise juhend

11.4.1. Kirjeldab häid tavasid IT-süsteemide talitluspidevuse plaanide jaoks, sealhulgas talitluspidevuse strateegia väljatöötamist, mõjuhindamist ja plaanide testimist.

11.5. ELi GDPR (2016/679)

11.5.1. Artikkel 32 – töötlemise turvalisus: nõuab töötlemissüsteemide vastupidavust ning isikuandmete käideldavuse ja neile juurdepääsu õigeaegset taastamist pärast intsidenti.

11.6. ELi NIS2 direktiiv (2022/2555)

11.6.1. Artikkel 21(2)(f): nõuab talitluspidevuse ja kriisiohje meetmeid võrgu- ja infosüsteemide turvalisuse toetamiseks.

11.7. ELi DORA (2022/2554)

11.7.1. Artikkel 10 – IKT talitluspidevus: nõuab finantssektori üksustelt IKT talitluspidevuse plaanide väljatöötamist ja testimist, sealhulgas riskipõhiseid RTO/RPO sihte ning ümberlülituse võimekust.

11.8. COBIT 2019

11.8.1. DSS04 – talitluspidevuse juhtimine: hõlmab kõiki talitluspidevuse planeerimise aspekte, sealhulgas ohtude tuvastamist, mõjuhindamist, taastestrateegiat ja regulaarset testimist.