					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P32S					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	Punktid 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontrollid 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
ELi GDPR	Artiklid 32, 33	
ELi NIS2	Artikkel 21(2)(f)	
ELi DORA	Artikkel 10	
COBIT 2019	DSS04	

1. Eesmärk

1.1 Käesolev poliitika tagab, et organisatsioon suudab säilitada äritegevuse toimepidevuse ja taastada olulised IT-teenused tegevushäirete ajal ja järel, sealhulgas elektrikatkestuste, küberrünnakute, lunavaranakkuste või süsteemitõrgete korral.

1.2 Käesolev poliitika kehtestab selge raamistiku talitluspidevuse ja katastroofitaaste (BC/DR) kavandamiseks, arvestades selliste VKE-de vajadusi, kellel puuduvad eraldiseisvad IT-meeskonnad.

1.3 Käesolev poliitika aitab organisatsioonil täita standarditest ISO/IEC 27001:2022, GDPR-ist, NIS2-st, DORA-st ja COBIT 2019-st tulenevaid kohaldatavaid nõudeid ning tugevdada talitluspidevust ja klientide usaldust.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõik ärikriitilised süsteemid ja teenused (nt e-post, pilvesalvestus, arveldusplatvormid, kliendiandmed)

2.1.2 kõik töötajad ja väline IT-teenuse osutaja, kes vastutavad BC/DR valmisoleku ja rakendamise eest

2.1.3 kõik häireolukorrad, sealhulgas küberintsidendid, riistvararikked, elektrikatkestused, üleujutused ja olukorrad, kus kontoriruumidele puudub juurdepääs

2.2 Poliitika hõlmab järgmist:

2.2.1 varunduse haldus

2.2.2 äritegevuse järjepidevuse plaanid (BCP)

2.2.3 katastroofitaaste tegevused

2.2.4 töötajate koolitus ja testimine

2.2.5 õiguslikud ja regulatiivsed reageerimisprotseduurid

3. Eesmärgid

3.1 Kaitsta organisatsiooni suutlikkust osutada võtmeteenuseid ka planeerimata häirete korral.

3.2 Tagada süsteemide ja andmete õigeaegne taaste eelnevalt määratletud taasteaja eesmärkide (RTO) alusel.

3.3 Võimaldada kõigil töötajatel kriisiolukorras järgida talitluspidevuse protseduure minimaalse segadusega.

3.4 Säilitada vastavus andmekaitse- ja talitluspidevuse nõuetele, sealhulgas GDPR-i artiklile 32 ja NIS2 artiklile 21.

3.5 Kehtestada praktiline ja testitav talitluspidevuse ning taastamise strateegia, mis sobib VKE-dele.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Vastutab BC/DR protsessi ja käesoleva poliitika rakendamise eest

4.1.2 Kinnitab äritegevuse järjepidevuse plaani (BCP)

4.1.3 Koordineerib häireolukordade ajal intsidendihaldust ja sisekommunikatsiooni

4.1.4 Esitab nõutavad regulatiivsed teavitused (nt GDPR-i kohased rikkumisteated)

4.2 IT-teenuse osutaja / süsteemiadministraator

4.2.1 Hoiab varukoopiad kasutuskõlblikuna ja testib neid

4.2.2 Käivitab vajaduse korral katastroofitaaste protseduurid

4.2.3 Dokumenteerib kõik taastetoimingud ja süsteemide taastamise sündmused

4.2.4 Teatab tegevjuhile viivitamata kriitilistest IT-intsidentidest

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Poliitika ja plaani iga-aastane läbivaatamine

9.1.1 Tegevjuht (GM) peab tagama, et käesolev poliitika ja sellega seotud äritegevuse järjepidevuse plaan (BCP) vaadatakse ametlikult läbi vähemalt üks kord aastas.

9.1.2 Läbivaatamine peab hõlmama vähemalt järgmist:

9.1.2.1 uute või esilekerkivate riskide hindamine

9.1.2.2 RTO-de ja RPO-de kordusvalideerimine

9.1.2.3 tarnijate ja kontaktandmete kontrollimine

9.1.2.4 kooskõla kontroll IT-süsteemide, õiguslike kohustuste või tegevuse muutustega

9.2 Sündmuspõhised ajakohastused

9.2.1 Käesolevat poliitikat tuleb ajakohastada ka järgmiste asjaolude ilmnemisel:

9.2.1.1 olulised intsidendid või häired, eriti juhul, kui eesmärke ei saavutatud

9.2.1.2 uued õiguslikud või regulatiivsed kohustused (nt DORA muudatused)

9.2.1.3 muudatused kriitilistes süsteemides, pilveplatvormides või personalis

9.2.1.4 iga-aastaste BCP/DR testide auditileiud

9.3 Muudatuste kontrolli protsess

9.3.1 Kõik muudatused peab kinnitama GM

9.3.2 Tuleb pidada versiooniajaloo logi, sealhulgas kuupäeva, muudatuse kirjelduse ja kinnitaja andmetega

9.3.3 Ajakohastatud poliitika tuleb uuesti edastada kõigile asjaomastele töötajatele, sealhulgas IT-teenuse osutajale ja osakonnajuhtidele

9.4 Saadud õppetundide dokumenteerimine

9.4.1 Pärast teste või tegelikke häireid tuleb dokumenteeritud õppetunnid võtta aluseks järgmiste muudatuste tegemisel

9.4.2 Need läbivaatused peavad hõlmama ka tarnijate toimivuse hindamist ja reageerimise piisavuse kontrolli

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on tihedalt seotud järgmiste VKE poliitikatega:

10.1.1 P1S – Infoturbepoliitika: määratleb kõrgetasemelised turbe-eesmärgid, mida talitluspidevuse ja taastamise praktikad peavad toetama.

10.1.2 P4S – Juurdepääsukontrolli poliitika: võimaldab ärikatkestuse stsenaariumides kasutajate juurdepääsuõiguste erakorralist tühistamist või taastamist.

10.1.3 P6S – Riskijuhtimise poliitika: loob aluse talitluspidevusega seotud riskide tuvastamiseks, hindamiseks ja prioriseerimiseks.

10.1.4 P8S – Infoturbeteadlikkuse koolitus: tagab, et töötajad on häireolukordades tegutsemiseks valmis ja mõistavad BCP-d.

10.1.5 P15S – Varundamise ja taastamise poliitika: sätestab konkreetsed tehnilised protseduurid andmete käideldavuse ja taaste kaitsmiseks.

10.1.6 P17S – Andmekaitse ja privaatsuspoliitika: tagab, et talitluspidevuse planeerimisel järgitakse isikuandmete kaitse nõudeid ja GDPR-i nii intsidentide ajal kui ka järel.

10.1.7 P22S – Logimise ja seire poliitika: toetab selliste sündmuste tuvastamist, mis võivad käivitada BC/DR protsessid, ning annab häirete järel kohtuekspertiisi jaoks auditijälje.

10.1.8 P30S – Intsidentidele reageerimise poliitika (P30): eelneb vahetult taastamisprotsessi aktiveerimisele küber- või tegevusintsidentide korral.

10.1.9 P31S – Tõendite kogumise ja kohtuekspertiisi poliitika: tagab, et talitluspidevuse stsenaariumides kogutakse digitaalsed tõendid vastavuse, kindlustuse või uurimise eesmärgil.

10.2 Need poliitikad moodustavad sidusa ja auditivalmis raamistiku vastupidavuse, vastutuse ja kontrollide järjepidevuse tagamiseks kõigis VKE tegevustes.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:

11.1.1 Punkt 6.1 – nõuab riskipõhist planeerimist ja riskikäsitlust, sealhulgas äritegevuse järjepidevust ja taastamist.

11.1.2 Punkt 6.3 – rõhutab pideva täiustamise põhimõtet pärast häireid.

11.1.3 Punkt 8.1 – nõuab tegevuste kavandamise ja ohje põhimõtteid, sealhulgas dokumenteeritud talitluspidevuse meetmeid.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.29 – nõuab äritegevuse järjepidevuse korralduse kehtestamist ja alalhoidmist.

11.2.2 Kontroll 5.30 – nõuab nende korralduste testimist ja läbivaatamist.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – määratleb talitluspidevuse planeerimise nõuded.

11.3.2 CP-4 – nõuab organisatsiooni töötajatele talitluspidevuse koolituse korraldamist.

11.3.3 CP-6 – käsitleb alternatiivse säilitamiskoha nõudeid.

11.3.4 CP-7 – sätestab alternatiivse töötluskoha ootused.

11.4 ELi GDPR:

11.4.1 Artikkel 32 – nõuab meetmeid töötlemissüsteemide ja -teenuste pideva käideldavuse ning vastupidavuse tagamiseks.

11.4.2 Artikkel 33 – käivitab teavitamiskohustuse juhul, kui talitluspidevuse puudulikkus põhjustab isikuandmete rikkumise.

11.5 ELi NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(f) – nõuab talitluspidevuse planeerimist ja kriisijuhtimise võimekust küberturvalisuse riskivalmiduse osana.

11.6 ELi DORA määrus (2022/2554):

11.6.1 Artikkel 10 – nõuab digitaalse tegevuskerksuse testimise ja taastamisvõimekuse rakendamist, eriti finantssektori VKE-de puhul.

11.7 COBIT 2019:

11.7.1 DSS04 – Talitluspidevuse juhtimine: annab juhtimissuunised talitluspidevuse säilitamiseks ja valideerimiseks, sealhulgas vastutuse, testimise, tarnijate kaasamise ja intsidendijärgsete läbivaatamiste kohta.