					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P15S					Dokumendi pealkiri: **Varundamise ja taastamise 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	Varundamise kontrollimeetmed vastavalt ISMS-i nõuetele
ISO/IEC 27002:2022	Kontrollid 5.29, 8	Varundamise head tavad ja lõimimine äritegevuse järjepidevusega
NIST SP 800-53 Rev. 5	CP-9, MP-6	Varundamine ja andmekandjate kaitse
ELi NIS2	Artikkel 21(2)(c)	Toimepidevus ja järjepidevus varundamise kaudu
ELi DORA	Artikkel 10(1)	IKT järjepidevus – varundamine finantssektori organisatsioonidele
COBIT 2019	BAI04.05, DSS04	Varukoopiate dokumenteerimine ja testimine ning protsesside kontroll
ELi GDPR	Artiklid 5(1)(f), 32(1)(c)	Andmete terviklus, käideldavus ja õigeaegne taastamine

1. Eesmärk

1.1 Käesolev poliitika sätestab, kuidas organisatsioon teostab ja haldab varundamist, et tagada talitluspidevus, kaitsta andmekao eest ning võimaldada intsidentidest õigeaegset taastumist.

1.2 Käesoleva poliitikaga kehtestatakse siduvad nõuded süsteemide ja andmete varundamiseks, säilitamiseks ning taastamiseks, eelkõige VKE-des, kus puudub keerukas IT-taristu.

1.3 Käesolev poliitika toetab auditivalmidust ja ISO/IEC 27001 sertifitseerimist, tagades, et olulised varundamise kontrollimeetmed on kehtestatud, neid rakendatakse järjepidevalt ning vaadatakse regulaarselt üle.

1.4 Organisatsiooni võime taastuda tehnilistest tõrgetest, juhuslikust kustutamisest või küberintsidentidest sõltub käesoleva poliitika rangest järgimisest.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigi ärisüsteemide ja andmete suhtes, sealhulgas:

2.1.1 finantsandmed, kliendiandmed ja personaliandmed

2.1.2 lauaarvutid, sülearvutid, serverid ja äriprotsessides kasutatavad pilverakendused

2.1.3 varunduskandjad, nagu USB-seadmed, välised andmekandjad või pilvekeskkonnas asuvad varukoopiad

2.2 Käesolev poliitika kehtib ka kõigi isikute suhtes, kes vastutavad varundamisprotsesside teostamise või haldamise eest, sealhulgas:

2.2.1 tegevjuht või muu määratud vastutav isik

2.2.2 välised IT-tugiteenuse osutajad või konsultandid

2.2.3 kõik töötajad, kes vastutavad andmete salvestamise eest heakskiidetud asukohtadesse

3. Eesmärgid

3.1 Tagada, et kõik kriitilised äriandmed ja süsteemid varundatakse turvaliselt asjakohaste ajavahemike järel, lähtudes riskist ja tegevusvajadusest.

3.2 Tagada, et andmeid saab häirete järel taastada õigeaegselt ja täielikult.

3.3 Ennetada varundusandmetele loata juurdepääsu, nende muutmist või kadu tõhusate säilitamise kontrollimeetmete abil.

3.4 Määratleda selgelt rollid ja vastutused varundus- ja taastamisprotseduuride rakendamisel ning testimisel ja tagada nende täitmine.

3.5 Toetada ISO/IEC 27001, GDPR-i ja muude õiguslike kohustuste täitmist struktureeritud ja dokumenteeritud varundamistavade kaudu.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 kiidab käesoleva poliitika heaks ja tagab selle rakendamise

4.1.2 eraldab ressursid ning määrab vastutuse varundamise ja taastamise tegevuste eest

4.1.3 vaatab läbi varundamise tõrked, intsidendid ja poliitikast kõrvalekalded

4.1.4 juhib poliitika iga-aastast läbivaatamist ja tagab auditivalmiduse

4.2 Väline IT-tugiteenuse osutaja (vajaduse korral)

4.2.1 rakendab ja haldab varunduslahendusi (kohapealseid või pilvepõhiseid)

4.2.2 jälgib varundamise õnnestumist ja kavandab taastamistestid

4.2.3 teatab tõrgetest ja intsidentidest otse tegevjuhile

4.2.4 tagab krüpteerimise, juurdepääsupiirangud ja varunduskandjate nõuetekohase käsitlemise

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb tegevjuhi poolt läbi vaadata vähemalt üks kord aastas. Vahepealse läbivaatamise alused on muu hulgas:

9.1.1 olulised muudatused süsteemides või säilitamismeetodites

9.1.2 uute pilve- või IT-platvormide kasutuselevõtt

9.1.3 õiguslikud või regulatiivsed muudatused, mis mõjutavad andmete taastamist

9.1.4 auditite või intsidentide tulemused

9.2 Tegevjuht vastutab läbivaatamise algatamise, muudatuste heakskiitmise ja uuenduste edastamise eest.

9.3 Poliitika versioone tuleb hallata ja arhiveerida. Kehtetuks muutunud versioonidele tuleb seada juurdepääsupiirangud, et vältida segadust auditite või äritegevuse taastamise sündmuste ajal.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on kooskõlas järgmiste VKE poliitikatega ja sõltub neist:

10.1.1 P14S – andmete säilitamise ja kõrvaldamise poliitika: määratleb, kui kaua tuleb varundusandmeid säilitada ja kuidas need turvaliselt kustutada.

10.1.2 P13S – andmete klassifitseerimise ja märgistamise poliitika: aitab seada prioriteete, millised andmed tuleb klassifitseerimistasemete alusel varundada.

10.1.3 P30S – intsidentidele reageerimise poliitika: käsitleb protseduure olukordadeks, kus varundamine ebaõnnestub või andmete taastamine on vajalik pärast rikkumist või katkestust.

10.1.4 P2S – juhtimisrollide ja vastutuste poliitika: määrab selge volituse varundamise järelevalveks ja poliitika rakendamiseks.

10.1.5 P17S – andmekaitse ja privaatsuse poliitika: tagab, et isikuandmete varundamisel järgitakse õiguslikke ja andmekaitsenõudeid.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1: varundussüsteemide operatiivne planeerimine ja kontroll ISMS-i osana

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.13: sätestab varundamise ajastamise, seire ja taastamise head tavad

11.2.2 Lisa A kontroll 5.29: käsitleb varundamise lõimimist äritegevuse järjepidevuse ja taastamisvalmidusega

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (talitluspidevuse planeerimine): määratleb struktureeritud varundusstrateegiad äritegevuse toimepidevuse tagamiseks

11.3.2 MP-6 (andmekandjate kaitse): nõuab varunduskandjate turvalist käsitlemist ja hävitamist

11.4 ELi GDPR

11.4.1 Artikkel 5(1)(f): nõuab isikuandmete tervikluse ja käideldavuse tagamist

11.4.2 Artikkel 32(1)(c): nõuab suutlikkust taastada juurdepääs isikuandmetele õigeaegselt

11.5 ELi NIS2 direktiiv

11.5.1 Artikkel 21(2)(c): nõuab varundamist ja taastamist toimepidevuse ning järjepidevuse planeerimise osana

11.6 ELi DORA

11.6.1 Artikkel 10(1): finantssektori organisatsioonid peavad tagama varundamise IKT järjepidevuse meetmete osana

11.7 COBIT 2019

11.7.1 BAI04.05: nõuab dokumenteeritud varundusstrateegiaid

11.7.2 DSS04.07: rõhutab regulaarset testimist ning kontrolli andmete varundamise ja taastamise protsesside üle