					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P15					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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1.3, 8	riskikäsitlus, planeerimine ja varundamise operatiivsed kontrollimeetmed
ISO/IEC 27002:2022	Kontrollimeetmed 8.13, 5.28, 5.29	varunduse haldus, toimepidevus ja turvaline kõrvaldamine
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	süsteemi varundamise, taastamise ja andmekandjate puhastamise nõuded
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32, põhjendus 49	isikuandmete taastamine ja käideldavus, talitluspidevus
ELi NIS2	Artikkel 21(2)(c-e)	varundamise ja talitluspidevuse kontrollimeetmed toimepidevuse tagamiseks
ELi DORA	Artiklid 10, 11	finantssektori varundamise, taastamise ja testimise nõuded
COBIT 2019	DSS01, DSS04, MEA03	varundamistoimingud, talitluspidevus ja vastavuse seire

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on kehtestada kohustuslikud nõuded andmete, süsteemide ja rakenduste varundamiseks ning taastamiseks, et toetada talitluspidevust, andmete terviklust ja äritegevuse järjepidevust.

1.2 Poliitika kehtestab standardiseeritud raamistiku, et:

1.2.1 kaitsta organisatsiooni andmeid kustutamisest, riknemisest, tõrgetest või küberrünnetest põhjustatud kao eest;

1.2.2 määratleda taaste-eesmärgid selgete RTO (taasteaja eesmärk) ja RPO (taastepunkti eesmärk) parameetrite kaudu;

1.2.3 lõimida varundamistoimingud laiemasse ISMS-i ning äritegevuse järjepidevuse ja katastroofitaaste plaanidesse (BCP/DRP);

1.2.4 tagada vastavus kohaldatavatele õigusaktidele ja valdkondlikele regulatsioonidele käideldavuse ning taastatavuse osas.

1.3 Poliitika rakendab ISO/IEC 27001:2022 kontrollimeetmeid, mis käsitlevad andmekandjate turvalist kõrvaldamist (5.28), infoturvet häiringu ajal (5.29) ja teabe varundamist (8.13), ning lähtub standardi ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR-i, DORA ja NIS2 headest tavadest.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmise suhtes:

2.1.1 kõik ISMS-i kohaldamisalasse kuuluvad ärikriitilised ja operatiivsed süsteemid;

2.1.2 kõik struktureeritud ja struktureerimata äriandmed, sealhulgas andmebaasid, failid, e-kirjad ja konfiguratsioonid;

2.1.3 kõik keskkonnad – kohapealsed, pilvepõhised, hübriidsed ning kaug- või välisasukohas asuvad salvestuslahendused;

2.1.4 kõik töötajad, kes vastutavad varundamisprotsesside haldamise, teostamise, kontrollimise või taastamise eest.

2.2 Poliitika kehtib ka järgmise suhtes:

2.2.1 varundusandmekandjad ja -taristu, sealhulgas füüsilised lindid, virtuaalsed seadmed, kettatõmmised ja pilvepõhised varunduslahendused;

2.2.2 kolmandatest osapooltest teenuseosutajad, kellega on sõlmitud leping organisatsiooni varukoopiate majutamiseks, haldamiseks või töötlemiseks;

2.2.3 logide, konfiguratsioonide, auditijälgede ja talitluspidevuse seisukohalt kriitilise operatiivse dokumentatsiooni varundamine.

2.3 Süsteemid, mis on varundamisest sõnaselgelt välja jäetud, tuleb dokumenteerida, nende kohta tuleb teha riskihindamine ning need peab ametlikult heaks kiitma infoturbe juht ja süsteemiomanik.

3. Eesmärgid

3.1 Tagada, et kõik kriitilised süsteemid ja andmed on usaldusväärselt varundatud piisava sageduse, liiasuse ja turbekontrollidega.

3.2 Tagada taastamismehhanismid, mis vastavad määratletud RTO ja RPO eesmärkidele kooskõlas ärimõju hinnangutega.

3.3 Säilitada täielik dokumentatsioon varundusprotseduuride, säilitusgraafikute, rollide ja tehnoloogiate kohta.

3.4 Valideerida varundamistoimingute tõhusus süstemaatilise taastamistestimise, tõrgete logimise ja parandusmeetmete jälgimise kaudu.

3.5 Kaitsta varundatud andmeid kogu nende elutsükli jooksul loata juurdepääsu, muutmise või hävitamise eest.

3.6 Tagada vastavus järgmisele:

3.6.1 ISO/IEC 27001 operatiivsete ja talitluspidevuse kontrollimeetmete nõuded;

3.6.2 NIST SP 800-53 CP- ja MP-perekondade varundamise ja puhastamise nõuded;

3.6.3 GDPR-i artikli 32 ja põhjenduse 49 nõuded isikuandmetele juurdepääsu taastamiseks;

3.6.4 DORA artikli 10 ja NIS2 artikli 21 nõuded IKT järjepidevusele ja toimepidevusele.

3.7 Tagada, et kolmandate osapoolte varundusteenused vastavad lepingulistele ja regulatiivsetele turbekohustustele, sealhulgas krüpteerimise, kõrvaldamise ja teavitamise protokollidele.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 kiidab käesoleva poliitika heaks ja tagab, et ärikriitilised süsteemid on piisavalt kaitstud heakskiidetud varundamise ja taastamise tavadega;

4.1.2 tagab, et varundamistoiminguteks on eraldatud piisavad ressursid ning nende vastavus õigusnormidele vaadatakse perioodiliselt läbi.

4.2 Infoturbejuht

4.2.1 vastutab käesoleva poliitika eest ja tagab selle kooskõla laiemate infoturbe-, riski- ja talitluspidevuse raamistikega;

4.2.2 teeb järelevalvet varundusprotseduuride lõimimise üle BCP/DRP-sse, intsidendihaldusse ja toimepidevuse planeerimisse;

4.2.3 vaatab läbi varundamise erandid ja hindab kriitiliste süsteemide välistamise riskide aktsepteerimise ettepanekuid.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord aastas või varem, kui selle käivitavad järgmised asjaolud:

9.1.1 muudatused äritegevuse järjepidevuse või katastroofitaaste strateegias;

9.1.2 uued regulatiivsed või õiguslikud kohustused, mis mõjutavad varundamise sagedust või andmete säilitamist;

9.1.3 muudatused süsteemiarhitektuuris, varundustööriistades või teenuseosutajates;

9.1.4 olulised intsidendid või auditileiud, mis on seotud andmekao või taaste ebaõnnestumistega.

9.2 Läbivaatamist koordineerib infoturbejuht koostöös järgmistega:

9.2.1 IT-taristu ja operatsioonid;

9.2.2 siseaudit;

9.2.3 andmekaitseametnik;

9.2.4 äritegevuse järjepidevuse ja katastroofitaaste meeskonnad.

9.3 Varundusgraafikud, süsteemide kaasamisloendid, taastamisdokumentatsioon ja erandilogid tuleb läbi vaadata paralleelselt, et tagada:

9.3.1 varundamise katvuse täpsus kõigi kriitiliste varade puhul;

9.3.2 vastavus RTO/RPO ja säilitamisnõuetele;

9.3.3 testimislogide ja intsidendiaruannete täielikkus;

9.3.4 varem tuvastatud kontrollimeetmete puuduste kõrvaldamine.

9.4 Kõik ajakohastused peavad:

9.4.1 olema versioonihaldusega ja säilitatud ISMS-i dokumentide hoidlas;

9.4.2 sisaldama muudatuste kokkuvõtet ja põhjendust;

9.4.3 olema tippjuhtkonna poolt heaks kiidetud;

9.4.4 olema teatavaks tehtud kõigile mõjutatud tehnilistele ja ärivaldkonna töötajatele.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetab otseselt järgmisi seotud dokumente ja on nendega seotud:

10.1.1 P6 - Riskijuhtimise poliitika: määratleb riskipõhise prioriseerimise süsteemide ja teenuste varunduskaitse jaoks.

10.1.2 P12 - Varahalduse poliitika: tagab, et varundamisele kuuluvad süsteemid on registreeritud ning seotud elutsükli jälgimise ja klassifitseerimisega.

10.1.3 P13 - Andmete klassifitseerimise ja märgistamise poliitika: suunab, millised andmekategooriad vajavad varundamist, sealhulgas prioriseerimist toetavaid märgistusmetaandmeid.

10.1.4 P14 - Andmete säilitamise ja kõrvaldamise poliitika: koordineerib varukoopiate säilitamist regulatiivsete säilitamispiirangute ja aegunud andmekandjate nõuetekohase kõrvaldamisega.

10.1.5 P16 - Andmete maskeerimise ja pseudonüümimise poliitika: toetab andmete minimeerimist tundlike andmekogumite varundamisel.

10.1.6 P30 - Intsidendidele reageerimise poliitika: rakendub varundamise tõrgete, taastamisprobleemide või varukoopiate andmehoidlate kompromiteerimise korral.

10.2 Need omavahel seotud poliitikad moodustavad ühtse raamistiku, mis tagab, et varundamise juhtimine on lõimitud organisatsiooni laiemasse ISMS-i ja operatiivse toimepidevuse strateegiasse.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:

11.1.1 Punkt 6.1.3 - riskikäsitluskava: toetab riskipõhist varundamise prioriseerimist ja taastamise planeerimist.

11.1.2 Punkt 8.1 - operatiivne planeerimine ja ohje: lõimib taastamise ja talitluspidevuse kontrollimeetmed operatiivsete kaitsemeetmete osana.

11.1.3 Lisa A kontrollimeede 5.28 - andmekandjate turvaline kõrvaldamine või korduskasutus: käsitleb varundusandmekandjate turvalist puhastamist.

11.1.4 Lisa A kontrollimeede 5.29 - infoturve häiringu ajal: tagab taastamisvõimekuse intsidentide või katastroofide ajal.

11.1.5 Lisa A kontrollimeede 8.13 - teabe varundamine: käsitletud otseselt kavandatud, testitud ja turvaliste varundamistoimingute kaudu.

11.2 ISO/IEC 27002:2022 - kontrollimeetmed 8.13, 5.28, 5.29: need kontrollimeetmed tugevdavad nõuet teha regulaarseid varukoopiaid, valideerida terviklust ja kavandada taastamist kõigis IT-keskkondades.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - süsteemi varundamine: kehtestab terviklikud varundusprotseduurid, sealhulgas välisasukohas salvestamise ja taastamistestimise.

11.3.2 CP-10 - süsteemi taastamine: nõuab valideeritud protseduure täielikuks või osaliseks taastamiseks kooskõlas taaste-eesmärkidega.

11.3.3 MP-6 - andmekandjate puhastamine: tagab aegunud varundusandmekandjate turvalise käitlemise.

11.3.4 SI-12 - teabe haldamise ja säilitamise protseduurid: tugevdab tundlike andmete varundamise ja taastamisega seotud vastutusi.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

11.4.1 Artikkel 32 - isikuandmete töötlemise turvalisus: nõuab taastamisvõimekust ja andmete käideldavuse kaitsemeetmeid, eelkõige isikuandmete puhul.

11.4.2 Põhjendus 49: toetab äritegevuse järjepidevuse ja katastroofitaaste meetmeid, sealhulgas turvalist varundamist organisatsiooni toimepidevuse osana.

11.5 ELi NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(c-e): nõuab tehnilisi ja korralduslikke meetmeid, sealhulgas varundamise ja talitluspidevuse kontrollimeetmeid, et tagada teenuste toimepidevus.

11.6 ELi DORA (2022/2554):

11.6.1 Artikkel 10 - IKT äritegevuse järjepidevus: nõuab finantsüksustelt täielikku andmete varundamist, taastamist ja talitluspidevuse planeerimist.

11.6.2 Artikkel 11 - IKT äritegevuse järjepidevuse plaanide testimine: rõhutab taastamisvõimekuse valideerimist regulaarse testimise kaudu.

11.7 COBIT 2019:

11.7.1 DSS01 - hallatud operatsioonid: toetab teenuste usaldusväärset osutamist kaitstud andmete käideldavuse kaudu.

11.7.2 DSS04 - hallatud talitluspidevus: määratleb strateegilised ja operatiivsed talitluspidevuse kontrollimeetmed, sealhulgas kontrollitud varukoopiad.

11.7.3 MEA03 - vastavuse seire, hindamine ja auditeerimine: nõuab talitluspidevuse meetmete, sealhulgas varundamise kontrollimeetmete tõhususe perioodilist läbivaatamist.