					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P05					Dokumendi pealkiri: **muudatuste juhtimise 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**

Kohaldatavate standardite ja regulatsioonidega kooskõlas

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 5.15	Käsitleb riskidega seotud tegevusi, pääsukontrolli ja muudatuste juhtimist
ISO/IEC 27002:2022	Kontroll 8	Rakendab struktureeritud muudatuste juhtimise protsessi
NIST SP 800-53 Rev.5	CM-2 kuni CM-14	Konfiguratsioonihalduse kontrollimeetmed
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 32(1)(b–d), 25; põhjendus 78	Süsteemide ja andmete turvalisuse tehnilised ja korralduslikud meetmed muudatuste ajal
ELi NIS2	Artikkel 21(2)(a, b, d, e)	Nõuab IKT muudatustega seotud riskide juhtimist
ELi DORA	Artiklid 5, 8, 12	Reguleerib tegevusriski ja IKT-riski juhtimist ning intsidentidest teavitamist
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Struktureeritud IT-muudatuste juhtimise toimivus, vastavus ja nõuded

1. Eesmärk

1.1. Käesolev poliitika kehtestab formaalse raamistiku organisatsiooni infosüsteemide, taristu, rakenduste ja nendega seotud protsesside muudatuste algatamiseks, hindamiseks, heakskiitmiseks, rakendamiseks ja läbivaatamiseks.

1.2. Sellega tagatakse, et kõik muudatused viiakse ellu kontrollitult ja auditijäljega, minimeerides katkestuste, turvalisuse halvenemise või õigusnormidele mittevastavuse riski.

1.3. Poliitika toetab standardi ISO/IEC 27001:2022 lisa A kontrolli 8.32 nõudeid, kehtestades turvalised, dokumenteeritud ja riskidega kooskõlas olevad muudatuste juhtimise praktikad.

1.4. Poliitika tagab ka muudatusotsuste jälgitavuse ning toetab talitluspidevust planeeritud ja erakorraliste muudatuste ajal.

2. Kohaldamisala

2.1. Käesolev poliitika kohaldub kõigile muudatustele, mis mõjutavad süsteeme, andmeid ja keskkondi ISMS-i kohaldamisalas, sealhulgas:

2.1.1. IT-taristu (kohapealne, pilvepõhine, hübriidne)

2.1.2. Tootmis-, eeltootmis- ja katastroofitaastekeskkonnad

2.1.3. Ärirakendused, teenused, API-d ja integratsioonid

2.1.4. Konfiguratsiooniseaded, süsteemipaigad, tarkvaraväljalasked ja süsteemide migreerimine

2.1.5. Erakorralised parandused ning projektipõhised või planeeritud muudatused

2.2. Poliitika reguleerib muudatusi, mille algatavad:

2.2.1. Sisemised töötajad (IT-operatsioonid, arendajad, süsteemiomanikud)

2.2.2. Välised tarnijad, hallatud teenusepakkujad (MSP-d) ja töövõtjad

2.2.3. Projektimeeskonnad süsteemide juurutamise, uuendamise või teenuse üleviimise käigus

2.3. Käesolev poliitika ei kohaldu:

2.3.1. Ajutistele testimis- või arenduskeskkondadele, millel puudub juurdepääs tootmisandmetele

2.3.2. Kasutajate isiklikele konfiguratsioonidele (käsitletud lubatud kasutuse poliitikas)

2.3.3. Muudatustele süsteemides, mis jäävad väljapoole organisatsiooni käsitlusala piire, välja arvatud juhul, kui need mõjutavad integreeritud varasid või vastavuskohustusi

3. Eesmärgid

3.1. Tagada, et kõik muudatused vaadatakse enne elluviimist läbi, kiidetakse heaks, testitakse ja dokumenteeritakse.

3.2. Säilitada muudatustega seotud tegevuste ajal ja järel süsteemide käideldavus, andmete terviklus ja teenuste järjepidevus.

3.3. Nõuda kõigi muudatustüüpide jaoks määratletud muudatuste klassifikatsioone, tagasipöördumisplaane ja riskihindamisi.

3.4. Võimaldada läbipaistvat otsustamist ja eskaleerimist struktureeritud juhtimise kaudu.

3.5. Toetada auditi valmidust jälgitavate muudatuskirjete ja rakendamisjärgsete ülevaatuste kaudu.

3.6. Tagada tööülesannete lahusus ja vähendada autoriseerimata või vastuoluliste muudatuste riski kriitilise tähtsusega süsteemides.

4. Rollid ja vastutused

4.1. Tippjuhtkond

4.1.1. Kinnitab muudatuste halduse poliitika ja tagab selle kooskõla strateegiliste eesmärkide ning regulatiivsete kohustustega.

4.1.2. Kiidab juhtimise järelevalve raames heaks suure mõjuga või valdkonnaülesed muudatusprogrammid.

4.1.3. Eraldab vajalikud ressursid ja eelarve muudatuste kontrolli tööriistade ning personali koolituse jaoks.

4.2. Muudatuste nõukogu

4.2.1. Vaatab läbi ja annab loa standard- ning suure mõjuga muudatustele, tagades riskide, mõju ja sõltuvuste asjakohase hindamise.

4.2.2. Valideerib tagasipöördumisplaanid, testitulemused, sidusrühmade teavitused ja ajastuse.

4.2.3. Koosseisu kuuluvad süsteemiomanike, infoturbe, IT-operatsioonide, ärijuhtimise ja vastavusfunktsiooni esindajad.

4.2.4. Võib dokumenteeritud tingimustel delegeerida otsuseid madala riskiga või erakorraliste muudatuste korral.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Läbivaatamise ajendid ja sagedus

9.1.1. Käesolev poliitika tuleb läbi vaadata kord aastas või järgmiste asjaolude ilmnemisel:

9.1.1.1. suuremad IT- või taristumuudatused

9.1.1.2. olulised intsidendid, mis on seotud ebaõnnestunud või autoriseerimata muudatustega

9.1.1.3. regulatiivsed muudatused või uued muudatustega seotud õiguslikud kohustused

9.1.1.4. uute tööriistade või CMS-platvormide kasutuselevõtt

9.2. Muudatuste halduse poliitika läbivaatamise protsess

9.2.1. Muudatuste haldur juhib läbivaatamise protsessi koostöös järgmiste osapooltega:

9.2.1.1. IT, infoturve ja operatsioonid

9.2.1.2. siseaudit ja riskijuhtimine

9.2.1.3. muudatuste nõukogu esindajad

9.2.2. Ajakohastused peavad läbi vaatama ja heaks kiitma tippjuhtkond ning infoturbe juhtimissüsteemi juhtkomitee.

9.2.3. Uuesti välja antud versioonid tuleb registreerida dokumendiregistris, neist tuleb mõjutatud osapooli teavitada ning vajaduse korral uuendada tutvumiskinnitusi.

9.3. Dokumendiohje ja versioonihaldus

9.3.1. Kõik versioonid peavad sisaldama:

9.3.1.1. poliitika ID-d, pealkirja ja klassifitseerimistaset

9.3.1.2. omanikku ja muudatuste ajalugu

9.3.1.3. muudatuste logi ja jõustumiskuupäeva

9.3.1.4. heakskiidu andjat

9.3.2. Arhiveeritud versioone tuleb säilitada kooskõlas dokumentide säilitamise poliitikaga (vähemalt 3 aastat).

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika on otseselt seotud järgmiste poliitikatega ja toetab nende rakendamist:

10.1.1. P1 – Infoturbe poliitika: kehtestab nõuded formaalsele infoturbe juhtimisele, turbekontrollidele ja protsessitaseme aruandekohustusele, sealhulgas muudatuste juhtimise osas.

10.1.2. P2 – Juhtimisrollide ja vastutuste poliitika: määratleb kinnitamisõigused ja tööülesannete lahususe, mis on asjakohased muudatuste autoriseerimise ja järelevalve jaoks.

10.1.3. P4 – Pääsukontrolli poliitika: tagab, et muudatuste elluviijate ja läbivaatajate juurdepääsuõigused järgivad vähimate õiguste põhimõtet.

10.1.4. P6 – Riskijuhtimise poliitika: tagab, et kõik muudatused alluvad asjakohasele riskihindamisele ja maandamismeetmetele.

10.1.5. P33 – Auditi ja vastavusseire poliitika: reguleerib muudatuste juhtimise kirjete ja rikkumiste valideerimist ning auditiülevaatust.

10.2. Need poliitikad koos võimaldavad ISMS-i raamistiku piires põhjendatava, jälgitava ja turvalise muudatuste juhtimise elutsükli.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001:2022

11.1.1. Punkt 6.1 – riskide ja võimaluste käsitlemise tegevused: käesolev poliitika toetab muudatustega seotud riskide tuvastamist, hindamist ja ohjamist.

11.1.2. Punkt 5.15 – pääsukontroll: tagab, et juurdepääs muudatuste ajal on kontrollitud ja jälgitav.

11.1.3. Lisa A kontroll 8.32 – muudatuste juhtimine: käesolev poliitika rakendab täielikult nõuet hallata infotöötlusvahendite ja süsteemide muudatusi planeeritud ja kontrollitud viisil.

11.2. ISO/IEC 27002:2022 – kontroll 8

11.2.1. Tugevdab struktureeritud muudatuste juhtimise protsessi rakendamist, sealhulgas muudatuste klassifikatsiooni, heakskiitu, testimist, tagasipöördumist ja dokumenteerimist.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM-perekond (CM-1 kuni CM-14): käesolev poliitika on tihedalt kooskõlas konfiguratsioonihalduse kontrollimeetmetega, sealhulgas baaskonfiguratsioonide (CM-2), konfiguratsioonimuudatuste kontrolli (CM-3), turvamõju analüüsi (CM-4) ja juurdepääsupiirangutega (CM-5).

11.3.2. AU-perekond (AU-2, AU-6, AU-12): käesolevas poliitikas viidatud logimis- ja auditimehhanismid toetavad sündmuste jälgitavust ja muudatustega seotud tegevuste vastavuse ülevaatust.

11.3.3. RA-3, RA-5: muudatustest tulenevad riskihindamised ja haavatavuse skaneerimised on lõimitud muudatuste hindamise protsessi.

11.3.4. PM-11 (missiooni-/äriprotsessi määratlus): tagab, et äritegevuse järjepidevus ja operatiivsed eesmärgid säilivad muudatuste ajal.

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

11.4.1. Artikkel 32(1)(b–d): käesolev poliitika toetab nõuet rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid andmete turvalisuse tagamiseks, eelkõige süsteemimuudatuste ajal.

11.4.2. Artikkel 25 – lõimitud andmekaitse ja vaikimisi andmekaitse: tagab, et isikuandmeid mõjutavad muudatused lõimivad andmekaitse ja turvalisuse kavandamisse ning juurutamisse.

11.4.3. Põhjendus 78: nõuab, et vastutavad töötlejad rakendaksid mehhanisme, näiteks muudatuste kontrolli poliitikaid, et tagada töötlemissüsteemide pidev konfidentsiaalsus, terviklus ja kerksus.

11.5. ELi NIS2 direktiiv (2022/2555)

11.5.1. Artikkel 21(2)(a, b, d, e): nõuab tehnilisi ja korralduslikke meetmeid IKT-riskide juhtimiseks, sealhulgas süsteemimuudatustest, tarkvarauuendustest ja taristumuudatustest tulenevate riskide korral.

11.6. ELi DORA (2022/2554)

11.6.1. Artikkel 5 – juhtimise ja sisekontrolli raamistik: käesolev poliitika kehtestab IKT muudatuste ja uuendustega seotud tegevusriski juhtimise põhimõtted.

11.6.2. Artikkel 8 – IKT riskijuhtimise raamistik: nõuab, et finantssektori üksused haldaksid kõiki IKT-süsteeme mõjutavaid muudatusi struktureeritud muudatuste juhtimise protsesside alusel, mida kajastavad ka käesoleva poliitika klassifikatsiooni-, testimis-, tagasipöördumis- ja dokumenteerimisnõuded.

11.6.3. Artikkel 12 – intsidentidest teavitamine: tagab, et ebaõnnestunud muudatused, mis põhjustavad IKT häireid, on jälgitavad, dokumenteeritud ja vajaduse korral raporteeritud.

11.7. COBIT 2019

11.7.1. BAI06 – hallatud IT-muudatused: käesolev poliitika täidab otseselt BAI06 eesmärke, kehtestades struktureeritud töövood muudatuste heakskiiduks, mõjuhindamiseks, teabevahetuseks ja testimiseks.

11.7.2. BAI02 – hallatud nõuete määratlemine ja BAI03 – hallatud lahenduste tuvastamine ning ülesehitus: tagavad, et ärivajadustest lähtuvad muudatused vaadatakse läbi ja rakendatakse turvaliselt.

11.7.3. DSS01 – hallatud operatsioonid: toetab süsteemide pidevat terviklust muudatuste elluviimise ajal.

11.7.4. MEA01 ja MEA03 – seire, hindamine ning toimivuse ja vastavuse hindamine: võimaldab muudatuste halduse poliitika tõhususe ja rakendamise pidevat järelevalvet.