					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P05S					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**

Kooskõla standardite ja regulatsioonidega

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 8	
ISO/IEC 27002:2022	Kontrollimeede 8	
NIST SP 800-53 Rev.5	CM-2 kuni CM-5, CM-11	
ELi NIS2	Artikkel 21(2)(b)	
ELi DORA	Artiklid 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on tagada, et kõik IT-süsteemide, konfiguratsioonide, ärirakenduste ja pilveteenuste muudatused kavandatakse, riskihinnatakse, testitakse ja kiidetakse heaks enne nende rakendamist.

1.2 Poliitika eesmärk on vähendada talitlushäireid, turvariske ja teenusekatkestusi, kehtestades lihtsustatud, kuid kohustusliku protsessi, mis sobib ka piiratud ressurssidega väikeettevõtetele.

1.3 Käesolev poliitika toetab ISO/IEC 27001:2022 sertifitseerimist, määratledes ametlikult, kuidas tehnilisi ja operatiivseid muudatusi hallatakse ja dokumenteeritakse.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmistele osapooltele:

2.1.1 töötajad ja osakonnajuhatajad, kes algatavad või viivad ellu muudatusi

2.1.2 välised IT-teenuse osutajad, kes haldavad süsteeme või tarkvara

2.1.3 tegevjuht, kes kannab üldvastutust muudatuste heakskiitmise eest

2.2 Poliitika hõlmab järgmiste objektide muudatusi:

2.2.1 tarkvara (uuendused, paikamised, uued rakendused)

2.2.2 riistvara (asendused, versiooniuuendused)

2.2.3 võrgu- ja tulemüürikonfiguratsioonid

2.2.4 pilveteenused, kasutajate juurdepääsuõigused ja tarnijate integratsioonid

2.2.5 infosüsteeme hõlmavad kriitiliste äriprotsesside muudatused

2.3 Käesoleva poliitika kohaldamisalasse kuuluvad nii kavandatud kui ka erakorralised muudatused.

3. Eesmärgid

3.1 Tagada, et kõik IT- ja ärisüsteemide muudatused on volitatud, dokumenteeritud ning probleemide ilmnemisel tagasi pööratavad.

3.2 Ennetada planeerimata seisakuid, andmekadu ja turbega seotud intsidente, mida põhjustavad kontrollimata muudatused.

3.3 Kehtestada lihtsad ja korratavad menetlused muudatuste esitamiseks, heakskiitmiseks, testimiseks ja tagasipööramiseks.

3.4 Säilitada auditikõlblik muudatuste logi, mis toetab operatiivset vastutust ja nõuetele vastavust.

3.5 Võimaldada riskipõhist otsustamist oluliste või tundlike muudatuste korral.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Kannab lõppvastutust kõigi oluliste muudatuste eest.

4.1.2 Vaatab läbi ja kiidab heaks mittestandardsed, kriitilised või kõrge riskiga muudatused.

4.1.3 Vaatab muudatuste logi läbi kord kvartalis või pärast olulisi intsidente.

4.2 IT-tugi või sisseostetud IT-teenuse osutaja

4.2.1 Viib muudatused ellu, sealhulgas konfiguratsiooniuuendused, paikamised ja süsteemide migratsioonid.

4.2.2 Peab lihtsustatud muudatuste logi, kuhu registreeritakse kuupäevad, muudatuse liigid, tulemused ja heakskiitjad.

4.2.3 Testib muudatusi enne rakendamist ja rakendab vajaduse korral tagasipööramistoimingud.

4.2.4 Teavitab mõjutatud kasutajaid enne ja pärast olulisi muudatusi.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane läbivaatamine

9.1.1 Tegevjuht või määratud IT-kontaktisik peab käesoleva poliitika vähemalt kord aastas läbi vaatama, et tagada selle kooskõla kehtivate süsteemide, töövoogude ja regulatiivsete nõuetega.

9.2 Vahepealsed läbivaatamised

9.2.1 Läbivaatamine tuleb algatada ka järgmistel juhtudel:

9.2.1.1 puudulikust muudatuste haldamisest põhjustatud turbeintsidendid

9.2.1.2 uute IT-süsteemide kasutuselevõtt

9.2.1.3 asjakohaste standardite, näiteks ISO, NIS2 või DORA, muudatused

9.3 Uuenduste dokumenteerimine

9.3.1 Käesoleva poliitika muudatused peavad olema versioonihallatud ja tegevjuhi poolt heaks kiidetud. Iga versioon peab sisaldama kuupäeva, muudatuste kokkuvõtet ja heakskiitjat.

9.4 Poliitikast teavitamine

9.4.1 Kõigist uuendustest tuleb teavitada kõiki mõjutatud töötajaid ja väliseid teenuse osutajaid. Dokumentatsioon tuleb ajakohastada kõigis viidatud asukohtades (nt töötajaportaal, ühiskettad).

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on tihedalt seotud järgmiste VKE poliitikatega:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb muudatuste heakskiitmise volitused.

10.1.2 P4S – Juurdepääsukontrolli poliitika: tagab, et muudatustest tulenevad juurdepääsuõiguste muudatused on dokumenteeritud ja korrektselt rakendatud.

10.1.3 P7S – Tööleasumise ja töösuhte lõpetamise poliitika: koordineerib rollimuudatuste ja juurdepääsude andmisega seotud muudatusi.

10.1.4 P15S – Varundamise ja taastamise poliitika: tagab, et tagasipööramise ja taastamise samme saab muudatuse nurjumise korral rakendada.

10.1.5 P30S – Intsidentidele reageerimise poliitika: määratleb, kuidas nurjunud või volitamata muudatusi käsitletakse turbeintsidentidena.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – riskipõhine planeerimine peab hõlmama muudatustega seotud tegevusi.

11.1.2 Punkt 8.1 – muudatustega seotud tegevustes tuleb teenuse tervikluse tagamiseks rakendada operatiivseid kontrollimeetmeid järjepidevalt.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 8.32 – annab suunised turvaliste muudatuste haldamise protsesside jaoks, sealhulgas dokumenteerimise, testimise ja heakskiitmise kohta.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – süsteemide baaskonfiguratsioon enne muudatust.

11.3.2 CM-3 – konfiguratsioonimuudatuste kontroll.

11.3.3 CM-4 – turbemõju analüüs.

11.3.4 CM-5 – muudatuste heakskiitmine ja dokumenteerimine.

11.3.5 CM-11 – muudatuste audit ja seire.

11.4 ELi NIS2 direktiiv

11.4.1 Artikkel 21(2)(b) – nõuab tehniliste ja korralduslike turvameetmete, sealhulgas muudatuste haldamise, ametlikke protseduure.

11.5 ELi DORA

11.5.1 Artiklid 6(9) ja 8(4)(b) – nõuavad, et finantssektori üksused rakendaksid IKT-süsteemide muudatuste ja konfiguratsioonide haldamist.

11.6 COBIT 2019

11.6.1 BAI06 – muudatuste haldamine: rõhutab planeerimist, riskide hindamist ja tagasipööramise võimekust.

11.6.2 DSS01 – operatsioonide haldamine: tagab operatiivse tervikluse tehniliste üleminekute ja muudatuste ajal.