					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P05S					Dokumenta nosaukums: **Izmaiņu pārvaldības politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)

(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.

Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.

Par licencēšanu sazinieties: info@clarysec.com

Saskaņotība ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 8. punkts	
ISO/IEC 27002:2022	8. kontroles pasākums	
NIST SP 800-53 Rev.5	CM-2 līdz CM-5, CM-11	
ES NIS2	21. panta 2. punkta b) apakšpunkts	
ES DORA	6. panta 9. punkts, 8. panta 4. punkta b) apakšpunkts	
COBIT 2019	BAI06, DSS	

1. Mērķis

1.1 Šī politika nosaka, ka visas izmaiņas IT sistēmās, konfigurācijās, darbības nodrošināšanai izmantotajās lietojumprogrammās vai mākoņpakalpojumos pirms ieviešanas ir jāplāno, jāizvērtē no riska viedokļa, jātestē un jāapstiprina.

1.2 Mērķis ir samazināt darbības traucējumus, drošības riskus un pakalpojumu nepieejamību, nosakot vienkāršotu, bet saistošu procesu, kas ir piemērots arī maziem uzņēmumiem ar ierobežotiem resursiem.

1.3 Šī politika atbalsta ISO/IEC 27001:2022 sertifikāciju, formalizējot tehnisko un operacionālo izmaiņu pārvaldību un dokumentēšanu.

2. Tvērums

2.1 Šī politika attiecas uz:

2.1.1 darbiniekiem un struktūrvienību vadītājiem, kuri ierosina vai īsteno izmaiņas;

2.1.2 ārējiem IT pakalpojumu sniedzējiem, kuri pārvalda sistēmas vai programmatūru;

2.1.3 ģenerāldirektoru, kurš ir vispārīgi atbildīgs par izmaiņu apstiprināšanu.

2.2 Tā aptver izmaiņas šādās jomās:

2.2.1 programmatūra (atjauninājumi, ielāpi, jaunas lietojumprogrammas);

2.2.2 aparatūra (nomaiņa, modernizācija);

2.2.3 tīkla un ugunsmūra konfigurācijas;

2.2.4 mākoņpakalpojumi, lietotāju piekļuves tiesības vai piegādātāju integrācijas;

2.2.5 darbībai kritisku procesu izmaiņas, kurās ir iesaistītas informācijas sistēmas.

2.3 Šīs politikas tvērumā ietilpst gan plānotas, gan ārkārtas izmaiņas.

3. Mērķi

3.1 Nodrošināt, ka visas IT un darbības sistēmu izmaiņas ir autorizētas, dokumentētas un atgriezeniskas problēmu gadījumā.

3.2 Novērst neplānotu dīkstāvi, datu zudumu vai drošības incidentus, ko izraisa nekontrolētas izmaiņas.

3.3 Noteikt vienkāršas un atkārtojamas procedūras izmaiņu iesniegšanai, apstiprināšanai, testēšanai un atcelšanai.

3.4 Uzturēt auditējamu izmaiņu žurnālu, kas nodrošina atbildību un atbilstību normatīvajām prasībām.

3.5 Nodrošināt uz risku balstītu lēmumu pieņemšanu būtisku vai sensitīvu izmaiņu gadījumā.

4. Lomas un atbildība

4.1 Ģenerāldirektors

4.1.1 Ir galīgi atbildīgs par visām būtiskajām izmaiņām.

4.1.2 Pārskata un apstiprina nerutīnas, kritiskas vai augsta riska izmaiņas.

4.1.3 Reizi ceturksnī vai pēc būtiskiem incidentiem pārskata izmaiņu žurnālu.

4.2 IT atbalsts vai ārpakalpojuma IT sniedzējs

4.2.1 Īsteno izmaiņas, tostarp konfigurāciju atjauninājumus, ielāpu uzstādīšanu un sistēmu migrāciju.

4.2.2 Uztur pamata izmaiņu žurnālu, kurā reģistrē datumus, izmaiņu veidus, rezultātus un apstiprinātājus.

4.2.3 Pirms ieviešanas testē izmaiņas un pēc vajadzības īsteno atcelšanas pasākumus.

4.2.4 Informē ietekmētos lietotājus pirms un pēc būtiskām izmaiņām.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā pārskatīšana

9.1.1 Šī politika ģenerāldirektoram vai norīkotajai IT kontaktpersonai ir jāpārskata reizi gadā, lai nodrošinātu tās atbilstību aktuālajām sistēmām, darba plūsmām un normatīvajām prasībām.

9.2 Starpposma pārskatīšana

9.2.1 Pārskatīšana ir jāierosina arī šādos gadījumos:

9.2.1.1 drošības incidenti, ko izraisījusi neatbilstoša izmaiņu pārvaldība;

9.2.1.2 jaunu IT sistēmu ieviešana;

9.2.1.3 izmaiņas attiecīgajos standartos, piemēram, ISO, NIS2 vai DORA.

9.3 Atjauninājumu dokumentēšana

9.3.1 Šīs politikas izmaiņas ir jāpārvalda, izmantojot versiju kontroli, un tās ir jāapstiprina ģenerāldirektoram. Katrā versijā ir jānorāda datums, izmaiņu kopsavilkums un apstiprinātājs.

9.4 Politikas paziņošana

9.4.1 Par visiem atjauninājumiem ir jāinformē visi ietekmētie darbinieki un ārējie pakalpojumu sniedzēji. Dokumentācija ir jāatjaunina visās atsauces vietās (piemēram, darbinieku portālā, koplietojamajos diskos).

10. Saistītās politikas un sasaistes

10.1 Šī politika ir cieši saistīta ar šādām SME politikām:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka pilnvaras izmaiņu apstiprināšanai.

10.1.2 P4S – Piekļuves kontroles politika: nodrošina, ka piekļuves izmaiņas, kas izriet no izmaiņām sistēmās, tiek pienācīgi dokumentētas un ieviestas.

10.1.3 P7S – Ievadīšanas amatā un darba attiecību izbeigšanas politika: koordinē izmaiņas, kas saistītas ar lomu maiņu un piekļuves piešķiršanu.

10.1.4 P15S – Rezerves kopēšanas un atjaunošanas politika: nodrošina, ka izmaiņu neveiksmes gadījumā var veikt atcelšanas un atjaunošanas darbības.

10.1.5 P30S – Incidentu reaģēšanas politika: nosaka, kā nesekmīgas vai neautorizētas izmaiņas tiek apstrādātas kā drošības incidenti.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 6.1. punkts – Uz risku balstītajā plānošanā ir jāietver izmaiņu darbības.

11.1.2 8.1. punkts – Ar izmaiņām saistītajām darbībām ir konsekventi jāpiemēro operacionālie kontroles pasākumi, lai nodrošinātu pakalpojumu integritāti.

11.2 ISO/IEC 27002

11.2.1 8.32. kontroles pasākums – Sniedz norādes drošiem izmaiņu pārvaldības procesiem, tostarp dokumentēšanai, testēšanai un apstiprināšanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – Sistēmu bāzlīnijas konfigurācija pirms izmaiņām.

11.3.2 CM-3 – Konfigurācijas izmaiņu kontrole.

11.3.3 CM-4 – Drošības ietekmes analīze.

11.3.4 CM-5 – Izmaiņu apstiprināšana un dokumentēšana.

11.3.5 CM-11 – Izmaiņu audits un uzraudzība.

11.4 ES NIS2 direktīva

11.4.1 21. panta 2. punkta b) apakšpunkts – Nosaka pienākumu ieviest formālas tehnisko un organizatorisko drošības pasākumu procedūras, tostarp izmaiņu pārvaldību.

11.5 ES DORA

11.5.1 6. panta 9. punkts un 8. panta 4. punkta b) apakšpunkts – Nosaka finanšu iestādēm pienākumu uzturēt IKT sistēmu izmaiņu un konfigurācijas pārvaldību.

11.6 COBIT 2019

11.6.1 BAI06 – Izmaiņu pārvaldība: uzsver plānošanu, riska izvērtēšanu un iespēju atcelt izmaiņas.

11.6.2 DSS01 – Operāciju pārvaldība: nodrošina darbības integritāti tehnisku pāreju un izmaiņu laikā.