					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P05					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**

Saskaņots ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1. punkts, 5. pielikums	Aptver riska apstrādes darbības, piekļuves kontroli un izmaiņu pārvaldību
ISO/IEC 27002:2022	8. kontrole	Ievieš strukturētu izmaiņu pārvaldības procesu
NIST SP 800-53 Rev.5	CM-2 līdz CM-14	Konfigurācijas pārvaldības kontroles pasākumi
ES GDPR	32. panta 1. punkta b)–d) apakšpunkts, 25. pants; 78. apsvērums	Tehniskie un organizatoriskie pasākumi sistēmu un datu drošībai izmaiņu laikā
ES NIS2	21. panta 2. punkta a), b), d), e) apakšpunkts	Nosaka IKT izmaiņu risku pārvaldību
ES DORA	5., 8. un 12. pants	Regulē operacionālo un IKT risku, kā arī incidentu ziņošanu
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Strukturēta IT izmaiņu pārvaldība, veiktspēja, atbilstība un prasības

1. Mērķis

1.1. Šī politika nosaka formālu ietvaru izmaiņu ierosināšanai, izvērtēšanai, apstiprināšanai, ieviešanai un pārskatīšanai organizācijas informācijas sistēmās, infrastruktūrā, lietojumprogrammās un saistītajos procesos.

1.2. Tā nodrošina, ka visas izmaiņas tiek īstenotas kontrolēti un auditējami, līdz minimumam samazinot darbības traucējumu, drošības apdraudējumu vai regulatīvās neatbilstības risku.

1.3. Tā atbalsta ISO/IEC 27001:2022 A pielikuma 8.32. kontroli, ieviešot drošas, dokumentētas un riskam atbilstošas izmaiņu pārvaldības prakses.

1.4. Politika nodrošina arī izmaiņu lēmumu izsekojamību un veicina operacionālo noturību plānotu vai ārkārtas izmaiņu laikā.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām izmaiņām, kas ietekmē sistēmas, datus un vides ISMS tvērumā, tostarp:

2.1.1. IT infrastruktūru (lokāli, mākoņvidē, hibrīdvidē)

2.1.2. ražošanas, pirmsražošanas un avārijas atjaunošanas vides

2.1.3. biznesa lietojumprogrammas, pakalpojumus, API un integrācijas

2.1.4. konfigurācijas iestatījumus, ielāpu uzstādīšanu, programmatūras laidienus un sistēmu migrāciju

2.1.5. ārkārtas labojumus un projektos balstītas vai plānotas izmaiņas

2.2. Tā reglamentē izmaiņas, ko ierosina:

2.2.1. iekšējais personāls (IT operācijas, izstrādātāji, sistēmu īpašnieki)

2.2.2. ārējie piegādātāji, pārvaldīto pakalpojumu sniedzēji (MSP), līgumslēdzēji un citi trešo pušu pakalpojumu sniedzēji

2.2.3. projektu komandas sistēmu ieviešanas, uzlabojumu vai pakalpojumu pārejas laikā

2.3. Šī politika neattiecas uz:

2.3.1. pagaidu testēšanas un izstrādes vidēm bez piekļuves ražošanas datiem

2.3.2. lietotāju personīgajām konfigurācijām (reglamentē Pieļaujamās izmantošanas politika)

2.3.3. izmaiņām sistēmās ārpus organizācijas kontroles robežām, izņemot gadījumus, kad tās ietekmē integrētos aktīvus vai atbilstības pienākumus

3. Mērķi

3.1. Nodrošināt, ka visas izmaiņas pirms izpildes tiek pārskatītas, apstiprinātas, testētas un dokumentētas.

3.2. Uzturēt sistēmu pieejamību, datu integritāti un pakalpojumu nepārtrauktību izmaiņu laikā un pēc tām.

3.3. Noteikt pienākumu visiem izmaiņu veidiem definēt izmaiņu klasifikāciju, izmaiņu atcelšanas plānus un riska novērtējumu.

3.4. Nodrošināt pārskatāmu lēmumu pieņemšanu un eskalāciju, izmantojot strukturētu pārvaldību.

3.5. Atbalstīt gatavību auditam ar izsekojamiem izmaiņu ierakstiem un pēcieviešanas pārskatīšanu.

3.6. Ieviest pienākumu nodalīšanu un samazināt nesankcionētu vai savstarpēji konfliktējošu izmaiņu risku kritiski svarīgās sistēmās.

4. Lomas un atbildība

4.1. Izpildvadība

4.1.1. Apstiprina Izmaiņu pārvaldības politiku un nodrošina tās atbilstību stratēģiskajiem mērķiem un regulatīvajiem pienākumiem.

4.1.2. Pārvaldības uzraudzības ietvaros apstiprina augstas ietekmes vai starpfunkcionālas izmaiņu programmas.

4.1.3. Piešķir nepieciešamos resursus un budžetu izmaiņu kontroles rīkiem un personāla apmācībai.

4.2. Izmaiņu konsultatīvā padome

4.2.1. Pārskata un apstiprina standarta izmaiņas un būtiskas izmaiņas, nodrošinot atbilstošu riska, ietekmes un savstarpējo atkarību izvērtēšanu.

4.2.2. Validē izmaiņu atcelšanas plānus, testēšanas rezultātus, ieinteresēto pušu komunikāciju un grafikus.

4.2.3. Tās sastāvā ir sistēmu īpašnieki, informācijas drošības, IT operāciju, biznesa vadības un atbilstības pārstāvji.

4.2.4. Tā var deleģēt lēmumus par zema riska vai ārkārtas izmaiņām dokumentētos apstākļos.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Pārskatīšanas ierosinātāji un biežums

9.1.1. Šī politika jāpārskata reizi gadā vai:

9.1.1.1. pēc būtiskām IT vai infrastruktūras izmaiņām

9.1.1.2. pēc nozīmīgiem incidentiem, kas saistīti ar neveiksmīgām vai nesankcionētām izmaiņām

9.1.1.3. pēc regulatīviem atjauninājumiem vai jaunām ar izmaiņām saistītām tiesiskām prasībām

9.1.1.4. ieviešot jaunus rīkus vai CMS platformas

9.2. Izmaiņu pārvaldības politikas pārskatīšanas process

9.2.1. Izmaiņu pārvaldnieks vada pārskatīšanas procesu sadarbībā ar:

9.2.1.1. IT, drošības un operāciju pārstāvjiem

9.2.1.2. iekšējo auditu un risku pārvaldību

9.2.1.3. Izmaiņu konsultatīvās padomes pārstāvjiem

9.2.2. Atjauninājumi jāpārskata un jāapstiprina izpildvadībai un Informācijas drošības vadības komitejai (ISSC).

9.2.3. Atkārtoti izdotās versijas jāuzskaita Dokumentu reģistrā un jāpaziņo skartajām pusēm, vajadzības gadījumā saņemot atkārtotu apliecinājumu.

9.3. Dokumentu kontrole un versiju pārvaldība

9.3.1. Visām versijām jāietver:

9.3.1.1. politikas ID, nosaukums un klasifikācijas līmenis

9.3.1.2. īpašnieks un pārskatījumu vēsture

9.3.1.3. izmaiņu žurnāls un spēkā stāšanās datums

9.3.1.4. apstiprināšanas pilnvaras

9.3.2. Arhivētās versijas jāglabā saskaņā ar Dokumentu glabāšanas politiku (vismaz 3 gadus).

10. Saistītās politikas un sasaistes

10.1. Šī politika ir tieši saistīta ar turpmāk minētajām politikām un atbalsta to ievērošanu:

10.1.1. P1 – Informācijas drošības politika: nosaka prasību formāliem drošības kontroles pasākumiem un procesu līmeņa pārskatatbildībai, tostarp izmaiņu pārvaldības pārraudzībai.

10.1.2. P2 – Pārvaldības lomu un atbildības politika: nosaka apstiprināšanas pilnvaras un pienākumu nodalīšanu, kas attiecas uz izmaiņu autorizēšanu un uzraudzību.

10.1.3. P4 – Piekļuves kontroles politika: nodrošina, ka piekļuves tiesības izmaiņu ieviesējiem un pārskatītājiem atbilst minimālo privilēģiju principam.

10.1.4. P6 – Risku pārvaldības politika: nodrošina, ka visām izmaiņām tiek veikta atbilstoša riska izvērtēšana un piemērotas riska mazināšanas stratēģijas.

10.1.5. P33 – Audita un atbilstības uzraudzības politika: reglamentē izmaiņu pārvaldības ierakstu un pārkāpumu validāciju, kā arī audita pārskatīšanu.

10.2. Šīs politikas kopumā nodrošina pamatotu, izsekojamu un drošu izmaiņu pārvaldības dzīves ciklu ISMS ietvarā.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001:2022

11.1.1. 6.1. punkts – Darbības risku un iespēju novēršanai: šī politika atbalsta ar izmaiņām saistīto risku identificēšanu, izvērtēšanu un kontroli.

11.1.2. 5.15. punkts – Piekļuves kontrole: nodrošina, ka piekļuve izmaiņu laikā ir kontrolēta un izsekojama.

11.1.3. A pielikuma 8.32. kontrole – Izmaiņu pārvaldība: šī politika pilnībā ievieš prasību plānoti un kontrolēti pārvaldīt izmaiņas informācijas apstrādes iekārtās un sistēmās.

11.2. ISO/IEC 27002:2022 – 8. kontrole

11.2.1. Stiprina strukturēta izmaiņu pārvaldības procesa ieviešanu, tostarp izmaiņu klasifikāciju, apstiprināšanu, testēšanu, izmaiņu atcelšanu un dokumentēšanu.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM saime (CM-1 līdz CM-14): šī politika ir cieši saskaņota ar konfigurācijas pārvaldības kontroles pasākumiem, tostarp bāzes konfigurāciju (CM-2), konfigurācijas izmaiņu kontroli (CM-3), drošības ietekmes analīzi (CM-4) un piekļuves ierobežojumiem (CM-5).

11.3.2. AU saime (AU-2, AU-6, AU-12): šajā politikā minētie žurnālfiksēšanas un uzraudzības kontroles pasākumi, kā arī audita mehānismi atbalsta notikumu izsekojamību un atbilstības pārskatīšanu ar izmaiņām saistītām darbībām.

11.3.3. RA-3, RA-5: izmaiņu izraisīta riska novērtēšana un ievainojamību skenēšana ir iekļauta izmaiņu izvērtēšanas procesā.

11.3.4. PM-11 (Misijas/biznesa procesu definēšana): nodrošina, ka izmaiņu laikā tiek saglabāta darbības nepārtrauktība un operacionālie mērķi.

11.4. ES GDPR (2016/679)

11.4.1. 32. panta 1. punkta b)–d) apakšpunkts: šī politika atbalsta prasību piemērot atbilstošus tehniskos un organizatoriskos pasākumus datu drošības nodrošināšanai, īpaši sistēmu izmaiņu laikā.

11.4.2. 25. pants – datu aizsardzība pēc projektēšanas un pēc noklusējuma: nodrošina, ka izmaiņās, kuras ietekmē personas datus, privātums un drošība tiek integrēti projektēšanā un ieviešanā.

11.4.3. 78. apsvērums: nosaka prasību, lai pārziņi ieviestu mehānismus, piemēram, izmaiņu kontroles politikas, nolūkā nodrošināt apstrādes sistēmu pastāvīgu konfidencialitāti, integritāti un noturību.

11.5. ES NIS2 direktīva (2022/2555)

11.5.1. 21. panta 2. punkta a), b), d), e) apakšpunkts: nosaka tehniskos un organizatoriskos pasākumus IKT risku pārvaldībai, tostarp riskus, kas rodas no sistēmu izmaiņām, programmatūras atjauninājumiem un infrastruktūras izmaiņām.

11.6. ES DORA (2022/2554)

11.6.1. 5. pants – Pārvaldības un iekšējās kontroles ietvars: šī politika ievieš operacionālā riska pārvaldības principus, kas saistīti ar IKT izmaiņām un atjauninājumiem.

11.6.2. 8. pants – IKT risku pārvaldības ietvars: nosaka, ka finanšu iestādēm visas izmaiņas, kas ietekmē IKT sistēmas, jāpārvalda strukturētos izmaiņu pārvaldības procesos, kas šajā politikā atspoguļoti klasifikācijas, testēšanas, izmaiņu atcelšanas un dokumentēšanas prasībās.

11.6.3. 12. pants – Incidentu ziņošana: nodrošina, ka neveiksmīgas izmaiņas, kas rada IKT traucējumus, ir izsekojamas, dokumentētas un, ja piemērojams, ziņojamas.

11.7. COBIT 2019

11.7.1. BAI06 – Pārvaldītas IT izmaiņas: šī politika tieši izpilda BAI06 mērķus, nosakot strukturētas darbplūsmas izmaiņu apstiprināšanai, ietekmes izvērtēšanai, komunikācijai un testēšanai.

11.7.2. BAI02 – Pārvaldīta prasību definēšana un BAI03 – Pārvaldīta risinājumu identificēšana un izveide: nodrošina, ka biznesa virzītas izmaiņas tiek pārskatītas un ieviestas droši.

11.7.3. DSS01 – Pārvaldītas operācijas: atbalsta nepārtrauktu sistēmu integritāti izmaiņu izpildes laikā.

11.7.4. MEA01 un MEA03 – Uzraudzīt, izvērtēt un novērtēt veiktspēju un atbilstību: nodrošina nepārtrauktu izmaiņu pārvaldības politikas efektivitātes un ievērošanas uzraudzību.