					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P33S					Dokumenta nosaukums: **Audita un atbilstības uzraudzības 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**

Saskaņotība ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	9.2. un 10. punkts	Iekšējie auditi, nepārtraukta pilnveide un neatbilstību novēršana
ISO/IEC 27002:2022	Kontroles pasākumi 5.35, 5.37	Plānota iekšējā pārskatīšana, neatkarīga ārpakalpojumu procesu pārskatīšana
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Drošības izvērtēšana, nepārtraukta uzraudzība, audita pārskatīšana, analīze un ziņošana
ES GDPR	24. un 32. pants	Tehnisko un organizatorisko pasākumu auditēšana, kontroles pasākumu efektivitātes apliecinājumi
ES NIS2	21. panta 2. punkta f) apakšpunkts	Proaktīva pārskatīšana un uz pierādījumiem balstīta atbilstība
ES DORA	10. pants	IKT risku pārvaldība, uzraudzība un ziņošana
COBIT 2019	MEA01, MEA03	Uzraudzība, atbilstības izvērtēšana, gatavība trešo pušu pārskatīšanai

1. Mērķis

1.1 Šī politika nosaka organizācijas pieeju iekšējo auditu veikšanai, drošības kontroles pasākumu pārbaudēm un regulatīvās atbilstības uzraudzībai. Tā nodrošina, ka visi kontroles pasākumi, politikas, sistēmas un pakalpojumu sniedzēji tiek regulāri un strukturēti pārskatīti.

1.2 Politikas mērķis ir identificēt kontroles pasākumu nepilnības, novērst neatbilstības un apliecināt pienācīgu rūpību saskaņā ar ISO/IEC 27001, GDPR un saistītajiem ietvariem.

1.3 Tā ļauj MVU uzturēt efektīvus darbības kontroles pasākumus un gatavību sertifikācijai arī bez atsevišķas atbilstības struktūrvienības, izmantojot vienkāršus, atkārtoti lietojamus kontrolsarakstus un uz risku balstītu konstatējumu prioritizēšanu.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām iekšējām struktūrvienībām un ārējiem pakalpojumu sniedzējiem, kuru pienākumi ir saistīti ar IT sistēmām, personas datiem un darbībai kritiskiem pakalpojumiem;

2.1.2 visiem kontroles pasākumiem un sistēmām, kas ietilpst informācijas drošības pārvaldības sistēmas darbības jomā;

2.1.3 visiem iekšējiem auditiem, drošības kontroles pasākumu pārskatīšanām un atbilstības pārbaudēm neatkarīgi no tā, vai tās veic organizācija, ārējais konsultants, klients vai regulators.

2.2 Šī politika attiecas arī uz pierādījumu vākšanu un ziņošanu saistībā ar:

2.2.1 ISO/IEC 27001 sertifikācijas un atkārtotās sertifikācijas auditiem;

2.2.2 datu aizsardzības auditiem saskaņā ar GDPR vai līguma noteikumiem;

2.2.3 klientu pieprasītām drošības anketām vai sākotnējās izpētes pārskatīšanām;

2.2.4 jebkurām regulatīvajām vai neatkarīgām pārskatīšanām saskaņā ar NIS2 vai DORA, ja tās ir piemērojamas.

3. Mērķi

3.1 Nodrošināt, ka visi galvenie kontroles pasākumi un politikas tiek regulāri pārskatīti attiecībā uz efektivitāti un atbilstību.

3.2 Uzturēt audita pierakstus un korektīvo darbību ierakstus, lai apliecinātu pārskatatbildību un pilnveidi.

3.3 Nodrošināt gatavību sertifikācijai, atkārtotai sertifikācijai un klientu apliecinājuma programmām, piemēram, ISO 27001 un piegādātāju izvērtēšanai.

3.4 Savlaicīgi identificēt nepilnības, lai nodrošinātu to operatīvu novēršanu, pirms tās eskalējas vai rada atbilstības pārkāpumus.

3.5 Nodrošināt ģenerāldirektoram un ārējam IT pakalpojumu sniedzējam iespēju koordinēt pārskatīšanas ar minimālu sarežģītību, vienlaikus saglabājot juridiski pamatotus rezultātus.

4. Lomas un atbildība

4.1 Ģenerāldirektors (GM)

4.1.1 pārrauga audita programmu;

4.1.2 apstiprina iekšējās pārskatīšanas plānus un konstatējumus;

4.1.3 nosaka korektīvās darbības un uzrauga to izpildi;

4.1.4 pilnvaro piesaistīt ārējos auditorus vai konsultantus.

4.2 IT pakalpojumu sniedzējs / administrators

4.2.1 nodrošina pierādījumus iekšējo un ārējo auditu laikā, piemēram, žurnālus, konfigurācijas un piekļuves kontroles ierakstus;

4.2.2 sniedz atbalstu tehnisko pārbaužu veikšanā, piemēram, attiecībā uz rezerves kopiju statusu un atbilstību ielāpu pārvaldības prasībām;

4.2.3 uztur audita pierādījumu repozitoriju.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Politikas un audita plāna ikgadējā pārskatīšana

9.1.1 Ģenerāldirektors (GM) pārskata šo politiku un audita grafiku vismaz reizi gadā.

9.1.2 Pārskatīšanā izvērtē:

9.1.2.1 auditu efektivitāti trūkumu identificēšanā;

9.1.2.2 auditu un korektīvo darbību izpildes līmeni;

9.1.2.3 izmaiņas piemērojamajās tiesiskajās, regulatīvajās vai sertifikācijas prasībās.

9.2 Uz ierosinošiem notikumiem balstīti atjauninājumi

9.2.1 Politika tiek pārskatīta un atjaunināta, ja:

9.2.2 sertifikācijas vai uzraudzības audits konstatē būtisku neatbilstību;

9.2.3 mainās tiesiskais vai regulatīvais ietvars, piemēram, tiek izdotas jaunas GDPR vadlīnijas vai notiek NIS2 ieviešana nacionālajā līmenī;

9.2.4 uzņēmējdarbības izmaiņas ietekmē sistēmas, procesus vai piegādātājus, kas ietilpst audita piemērošanas jomā;

9.2.5 kritisks incidents vai pārkāpums atklāj iepriekš nekonstatētus kontroles pasākumu trūkumus.

9.3 Atjauninājumu dokumentēšana

9.3.1 Visi grozījumi jāuzskaita politikas versiju kontroles žurnālā.

9.3.2 Atjauninājumi jāizplata visiem komandas locekļiem, kuri ir iesaistīti auditos.

9.3.3 Lai nodrošinātu izpratni, kopā ar atjaunināto politiku iekļauj izmaiņu kopsavilkumu.

10. Saistītās politikas un sasaiste

10.1 Šo politiku atbalsta un papildina vairākas citas MVU politikas:

10.1.1 P1S – Informācijas drošības politika: nosaka bāzes līmeni visām kontroles pasākumu prasībām un paredz to ievērošanas pārbaudi auditos.

10.1.2 P2S – Pārvaldības lomu un atbildības politika: nosaka pārskatatbildību par audita plānošanu, izpildi un atbildību par korektīvajām darbībām.

10.1.3 P6S – Risku pārvaldības politika: identificē auditos atklātos kontroles pasākumu trūkumus un nodrošina, ka konstatējumi tiek dokumentēti risku reģistrā.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nosaka GDPR kontroles pasākumus, kas ir auditējami, tostarp datu apstrādi, reaģēšanu uz pārkāpumiem un privātuma paziņojumus.

10.1.5 P22S – Žurnalēšanas un uzraudzības politika: nodrošina audita žurnālus un digitālās kriminālistikas pierādījumus, ko izmanto atbilstības un kontroles pasākumu pārskatīšanā.

10.1.6 P30S – Incidentu reaģēšanas politika: paredz periodisku incidentu ierakstu un pēcincidenta pārskatīšanu, lai pārbaudītu reaģēšanas efektivitāti.

10.1.7 P31S – Pierādījumu vākšanas un digitālās kriminālistikas politika: nosaka procedūras pārbaudāmu pierādījumu vākšanai un pierādījumu glabāšanas ķēdes nodrošināšanai auditu laikā.

10.2 Kopā šīs politikas veido noslēgtu kontroles vidi, kas nodrošina iekšējo verificēšanu, ārējo apliecinājumu un pārvaldību atbilstoši standartiem.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 9.2. punkts – nosaka prasību veikt iekšējos auditus, lai izvērtētu IDPS veiktspēju un atbilstību prasībām.

11.1.2 10.1. punkts – nosaka pienākumu nodrošināt nepārtrauktu pilnveidi, pamatojoties uz audita rezultātiem un neatbilstību novēršanu.

11.2 ISO/IEC 27002:

11.2.1 5.35. kontrole – nosaka prasību veikt plānotu kontroles pasākumu un procesu iekšējo pārskatīšanu.

11.2.2 5.37. kontrole – uzsver neatkarīgas pārskatīšanas nozīmi, īpaši attiecībā uz ārpakalpojumu procesiem.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Drošības izvērtēšana: nosaka prasību auditēt ieviestos kontroles pasākumus, lai pārbaudītu to efektivitāti.

11.3.2 CA-7 – Nepārtraukta uzraudzība: uzsver proaktīvu kontroles pasākumu nepilnību atklāšanu un pārskatīšanu.

11.3.3 AU-6 – Audita pārskatīšana, analīze un ziņošana: nosaka prasību regulāri analizēt un novērst problēmas, kas konstatētas audita žurnālos un konstatējumos.

11.4 ES GDPR:

11.4.1 24. un 32. pants – nosaka prasību ieviest un auditēt tehniskos un organizatoriskos pasākumus, tostarp nodrošināt kontroles pasākumu efektivitātes pierādījumus un to pilnveidi laika gaitā.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 20.–21. pants – nosaka pienākumu nodrošināt proaktīvu kontroles pasākumu pārskatīšanu, uz pierādījumiem balstītu atbilstību un auditējamību būtiskām un svarīgām vienībām.

11.6 COBIT 2019:

11.6.1 MEA01 – Veiktspējas un atbilstības uzraudzība, izvērtēšana un novērtēšana: nosaka prasību periodiski izvērtēt procesu un kontroles pasākumu veiktspēju attiecībā pret standartiem un mērķiem.

11.6.2 MEA03 – Atbilstības nodrošināšana ārējām prasībām: koncentrējas uz iekšējo uzraudzību un gatavību trešo pušu auditiem un regulatīvajām pārskatīšanām.