					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P33					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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontroles pasākumi 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
Vispārīgā datu aizsardzības regula (VDAR)	Panti 24, 32, 33	
NIS2	Pants 21(2)(g), 27	
DORA	Panti 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Mērķis

1.1 Šīs politikas mērķis ir noteikt un pārvaldīt organizācijas audita un atbilstības uzraudzības programmu, lai:

1.1.1 validētu drošības un privātuma kontroles pasākumu efektivitāti;

1.1.2 nodrošinātu atbilstību piemērojamajiem standartiem, normatīvajam regulējumam un līgumiskajām saistībām;

1.1.3 savlaicīgi identificētu neatbilstības, neefektivitāti un atbilstības riskus;

1.1.4 atbalstītu nepārtrauktu pilnveidi un gatavību sertifikācijām, izvērtējumiem un normatīvo prasību pārskatīšanai.

1.2 Šī politika atbalsta informācijas drošības pārvaldības sistēmas briedumu un integritāti, IDPS ietvaros nostiprinot strukturētu, uz risku un pierādījumiem balstītu audita un uzraudzības praksi.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām iekšējām biznesa vienībām, funkcijām un struktūrvienībām;

2.1.2 fiziskajiem objektiem, mākoņvidēm, SaaS platformām un ārpakalpojumiem;

2.1.3 informācijas sistēmām, lietojumprogrammām, infrastruktūru un datu aktīviem, ko pārvalda IDPS;

2.1.4 darbiniekiem, līgumslēdzējiem un trešo pušu pakalpojumu sniedzējiem, kuriem ir audita vai atbilstības pienākumi.

2.2 Politika aptver:

2.2.1 iekšējo auditu;

2.2.2 ārējos un sertifikācijas auditus;

2.2.3 tehnisko atbilstības uzraudzību;

2.2.4 piegādātāju un trešo pušu auditus;

2.2.5 korektīvās un preventīvās darbības (CAPA);

2.2.6 metriku, paneļus un ziņošanas procesus.

2.3 Tā attiecas uz visiem organizācijai saistošajiem ietvariem, tostarp ISO/IEC 27001, VDAR, NIS2, DORA un SOC 2, kā arī citiem piemērojamiem ietvariem.

3. Mērķi

3.1 Pārbaudīt IDPS un saistītajās vidēs ieviesto kontroles pasākumu, politiku un procedūru pietiekamību un efektivitāti.

3.2 Identificēt un novērst jebkādas nepilnības, neatbilstības vai atbilstības trūkumus, pirms tie izraisa incidentus vai pārkāpumus.

3.3 Nodrošināt pastāvīgu gatavību iekšējām vadības pārskatīšanām, ārējiem auditiem un neatkarīgām sertifikācijām.

3.4 Nodrošināt juridiski pamatotus pierādījumus un audita pēdas normatīvo iestāžu pieprasījumu, tiesvedību vai klientu apliecinājuma pieprasījumu vajadzībām.

3.5 Integrēt audita rezultātus organizācijas kopējā risku pārvaldībā, drošības metrikās un nepārtrauktas pilnveides aktivitātēs.

4. Lomas un pienākumi

4.1 Iekšējā audita vadītājs / atbilstības vadītājs

4.1.1 Plāno, sastāda grafiku un veic iekšējos auditus atbilstoši risku prioritātēm.

4.1.2 Uztur audita reģistru, koordinē audita darbības un uzrauga korektīvo darbību izpildi.

4.2 Galvenais informācijas drošības vadītājs (CISO)

4.2.1 Nodrošina, ka audita piemērošanas joma aptver visus būtiskos IDPS elementus un A pielikuma kontroles pasākumus.

4.2.2 Pārrauga CAPA validāciju un integrē audita rezultātus drošības programmā.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā atbilstības vadītājam un CISO vai agrāk, reaģējot uz:

9.1.1 izmaiņām regulatīvajos, līgumiskajos vai sertifikācijas ietvaros;

9.1.2 būtiskiem audita konstatējumiem vai atkārtotām kontroles pasākumu atteicēm;

9.1.3 organizatoriskām pārmaiņām vai GRC sistēmas izmaiņām;

9.1.4 ārējo auditoru ieteikumiem vai regulatoru atsauksmēm.

9.2 Pārskatīšanas procesā jāizvērtē:

9.2.1 audita plānošanas metodoloģija un biežums;

9.2.2 izmaiņas IDPS darbības jomā vai infrastruktūrā;

9.2.3 atjauninājumi kontroles katalogā vai tiesisko prasību reģistrā;

9.2.4 audita pierādījumu un CAPA procesu konsekvence un kvalitāte.

9.3 Visām politikas izmaiņām jābūt:

9.3.1 dokumentētām repozitorijā, kas tiek pārvaldīts ar versiju kontroli;

9.3.2 apstiprinātām izpildvadībā;

9.3.3 paziņotām visam ietekmētajam personālam un integrētām atjauninātajās procedūrās un informētības programmās.

9.4 Pēc pārskatīšanas veiktajai validācijai jāapstiprina, ka atjauninātās prasības ir atspoguļotas audita reģistrā, atbilstības rīkos un iekšējos uzraudzības paneļos.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir saskaņota ar šādām saistītajām organizācijas politikām:

10.1.1 P1 – Informācijas drošības politika: nosaka IDPS un izveido pārskatatbildību par atbilstību un nepārtrauktu pilnveidi;

10.1.2 P5 – Izmaiņu pārvaldības politika: nodrošina audita pārredzamību attiecībā uz infrastruktūras un konfigurācijas izmaiņām, kas ietekmē kontroles vidi;

10.1.3 P6 – Risku pārvaldības politika: integrē audita rezultātus organizācijas risku izvērtēšanā un riska apstrādes darbībās;

10.1.4 P14 – Datu glabāšanas un dzēšanas politika: nosaka audita pierādījumu, žurnālu un atbilstības ierakstu glabāšanu;

10.1.5 P18 – Kriptogrāfisko kontroles pasākumu politika: atbalsta sensitīvu audita datu drošu glabāšanu un pārsūtīšanu;

10.1.6 P26 – Trešo pušu un piegādātāju drošības politika: aptver audita tiesības, apliecinājuma dokumentus un piegādātāju atbilstības uzraudzību;

10.1.7 P30 – Reaģēšanas uz incidentiem politika: saskaņo incidentu apstrādes procesa auditus ar IDPS apliecinājuma mērķiem;

10.1.8 P32 – Darbības nepārtrauktības un avārijas atjaunošanas politika: nosaka prasību audita ciklu laikā pārbaudīt darbības nepārtrauktības testēšanu un atbilstību DRP.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiskajiem standartiem un tiesiskajām prasībām audita veikšanai un nepārtrauktai atbilstības validācijai.

11.2 ISO/IEC 27001:

11.2.1 Punkts 9.2 – Iekšējais audits: nosaka prasību regulāri veikt uz risku balstītus IDPS auditus, lai izvērtētu efektivitāti un atbilstību.

11.2.2 Punkts 9.3 – Vadības pārskatīšana: audita rezultāti jāintegrē stratēģiskajā pārskatīšanā un pilnveidē.

11.2.3 Punkts 10.1 – Neatbilstība un korektīvā darbība: audita konstatējumi jānovērš, izmantojot dokumentētas CAPA procedūras.

11.3 ISO/IEC 27002:2022 – kontroles pasākumi 5.35–5.37:

11.3.1 A pielikuma kontroles pasākumi 5.35–5.37: aptver neatkarīgu pārskatīšanu, atbilstību tiesiskajām un līgumiskajām prasībām un audita žurnālu veidošanu.

11.3.2 Tie sniedz ieviešanas vadlīnijas audita un atbilstības programmu plānošanai, izpildei un pilnveidei.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontroles pasākumu izvērtēšana: nosaka prasību regulāri pārskatīt ieviestos drošības kontroles pasākumus.

11.4.2 CA-5 – Rīcības plāns un starpposma mērķi (POA&M): atbilst audita konstatējumu uzskaitei un novēršanai.

11.4.3 CA-7 – Nepārtraukta uzraudzība: atbalsta proaktīvu, automatizētu atbilstības izvērtēšanu.

11.5 Vispārīgā datu aizsardzības regula (VDAR) (2016/679):

11.5.1 Panti 24 un 32: nosaka prasību, izmantojot atbilstošas pārvaldības struktūras, nodrošināt pierādījumus par drošības kontroles pasākumu ieviešanu un efektivitāti.

11.5.2 Pants 33: pamato nepieciešamību nodrošināt validētas audita pēdas incidentu un personas datu aizsardzības pārkāpumu reakcijai un paziņošanai.

11.6 NIS2 direktīva (2022/2555):

11.6.1 Pants 21(2)(g): nosaka politiku un procedūru auditēšanu kā daļu no minimālajiem kiberdrošības riska pārvaldības pasākumiem.

11.6.2 Pants 27: valsts kompetentās iestādes var veikt vai pieprasīt auditus būtiskām un svarīgām vienībām.

11.7 DORA (2022/2554):

11.7.1 Pants 10(2)(e): nosaka, ka vienībām jāveic IKT risku pārvaldības prakšu iekšējie un ārējie auditi.

11.7.2 Pants 25 – Audita prasības: nosaka periodiskus auditus, ko veic iekšējie vai neatkarīgi ārējie auditori, nodrošinot regulatoru pārredzamību.

11.8 COBIT 2019:

11.8.1 MEA01 – Uzraudzīt, izvērtēt un novērtēt veiktspēju un atbilstību: nodrošina, ka kontroles pasākumu efektivitāte tiek pārbaudīta un par to tiek ziņots pārvaldības institūcijām.

11.8.2 MEA03 – Uzraudzīt, izvērtēt un novērtēt atbilstību: nosaka organizācijas prakšu saskaņošanu ar tiesiskajām, līgumiskajām un standartos balstītajām prasībām.