| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | |
| Dokumendi number:<br>P33 | | | | | Dokumendi pealkiri:<br>**Auditi ja vastavusseire poliitika** | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>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/õigusnorm | Punkt/artikkel | Kommentaar |
|---|---|---|
| ISO/IEC 27001:2022 | Punktid 9.2, 9.3, 10 | |
| ISO/IEC 27002:2022 | Kontrollimeetmed 5.35–5.37 | |
| NIST SP 800-53 Rev.5 | CA-2, CA-5, CA-7 | |
| EL GDPR | Artiklid 24, 32, 33 | |
| EL NIS2 | Artikkel 21(2)(g), 27 | |
| EL DORA | Artiklid 10(2)(e), 25 | |
| COBIT 2019 | MEA01, MEA03 | |

## 1. Eesmärk

**1.1 Käesoleva poliitika eesmärk on kehtestada ja hallata organisatsiooni auditi- ja vastavusseire programmi, et:**

1.1.1 valideerida turbe- ja andmekaitsekontrollide tõhusus;

1.1.2 tagada vastavus kohaldatavatele standarditele, õigusraamistikele ja lepingulistele kohustustele;

1.1.3 tuvastada mittevastavused, ebatõhusused ja vastavusriskid õigeaegselt;

1.1.4 toetada pidevat täiustamist ning valmisolekut sertifitseerimisteks, hindamisteks ja regulatiivseteks läbivaatusteks.

1.2 Käesolev poliitika toetab infoturbe juhtimissüsteemi (ISMS) terviklust ja küpsust, lõimides sellesse struktureeritud, riskipõhised ja tõenduspõhised auditi- ning seirepraktikad.

## 2. Kohaldamisala

**2.1 Käesolev poliitika kohaldub järgmistele üksustele ja valdkondadele:**

2.1.1 sisemised äriüksused, funktsioonid ja osakonnad;

2.1.2 füüsilised tegevuskohad, pilvekeskkonnad, SaaS-platvormid ja sisseostetavad teenused;

2.1.3 infosüsteemid, rakendused, taristu ja andmevarad, mida hallatakse ISMS-i raames;

2.1.4 töötajad, töövõtjad ja kolmandatest osapooltest teenuseosutajad, kellel on auditist või vastavusest tulenevad kohustused.

**2.2 Poliitika hõlmab järgmist:**

2.2.1 siseaudit;

2.2.2 välisauditid ja sertifitseerimisauditid;

2.2.3 tehniline vastavusseire;

2.2.4 tarnijate ja kolmandate osapoolte auditid;

2.2.5 parandus- ja ennetusmeetmed (CAPA);

2.2.6 mõõdikud, juhtpaneelid ja aruandlusprotsessid.

2.3 Poliitika kohaldub kõigile asjakohastele raamistikele, mille nõuetele organisatsioon peab vastama, sealhulgas ISO/IEC 27001, GDPR, NIS2, DORA ja SOC 2.

## 3. Eesmärgid

3.1 Kontrollida ISMS-is ja sellega seotud keskkondades rakendatud kontrollimeetmete, poliitikate ja protseduuride piisavust ning tõhusust.

3.2 Tuvastada ja kõrvaldada puudused, mittevastavused või vastavuslüngad enne nende eskaleerumist intsidentideks või rikkumisteks.

3.3 Tagada püsiv valmisolek sisemisteks juhtkonna ülevaatusteks, välisaudititeks ja sõltumatuteks sertifitseerimisteks.

3.4 Luua kaitstav tõendusmaterjal ja auditijälg regulatiivsete päringute, õiguslike menetluste või klientide ja partnerite kinnitustaotluste toetamiseks.

3.5 Lõimida audititulemused organisatsiooni laiemasse riskijuhtimisse, infoturbe võtmetulemusnäitajate raamistikku ja pideva täiustamise tegevustesse.

**4. Rollid ja vastutused**

**4.1 Siseauditi juht / vastavusjuht**

4.1.1 Kavandab, ajastab ja viib siseauditeid läbi riskiprioriteetide alusel.

4.1.2 Hoiab auditiregistri ajakohasena, koordineerib audititegevusi ja jälgib parandusmeetmete täitmist.

**4.2 Infoturbe juht**

4.2.1 Tagab, et auditi kohaldamisala hõlmab kõiki asjakohaseid ISMS-i elemente ja lisa A kontrollimeetmeid.

4.2.2 Teostab järelevalvet CAPA valideerimise üle ja lõimib audititulemused turbeprogrammi.

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

**9. Läbivaatamise ja ajakohastamise nõuded**

**9.1 Vastavusjuht ja infoturbe juht peavad käesoleva poliitika läbi vaatama vähemalt kord aastas või varem, kui esineb üks järgmistest asjaoludest:**

9.1.1 muudatused regulatiivsetes, lepingulistes või sertifitseerimisraamistikes;

9.1.2 olulised auditileiud või korduvad kontrollimeetmete rikked;

9.1.3 organisatsioonilised ümberkorraldused või muudatused GRC-süsteemis;

9.1.4 välisaudiitori soovitused või regulaatori tagasiside.

**9.2 Läbivaatamise käigus tuleb hinnata vähemalt järgmist:**

9.2.1 auditi planeerimise metoodika ja sagedus;

9.2.2 muudatused ISMS-i kohaldamisalas või taristus;

9.2.3 kontrollikataloogi või õigusregistri ajakohastused;

9.2.4 auditităendite ja CAPA-protsesside järjepidevus ning kvaliteet.

**9.3 Kõik poliitikamuudatused peavad olema:**

9.3.1 dokumenteeritud versioonihaldusega repositooriumis;

9.3.2 kinnitatud tippjuhtkonna poolt;

9.3.3 edastatud kõigile mõjutatud töötajatele ning lõimitud ajakohastatud protseduuridesse ja teadlikkuse tõstmise programmidesse.

9.4 Läbivaatamisjärgne valideerimine peab kinnitama, et ajakohastatud nõuded kajastuvad auditiregistris, vastavustööriistades ja sisemistes seire juhtpaneelides.

**10. Seotud poliitikad ja seosed**

**10.1 Käesolev poliitika on kooskõlas järgmiste organisatsiooni seotud poliitikatega:**

10.1.1 P1 – Infoturbepoliitika: määratleb ISMS-i ja kehtestab vastutuse vastavuse ning pideva täiustamise eest;

10.1.2 P5 – Muudatuste haldamise poliitika: tagab auditi nähtavuse taristu- ja konfiguratsioonimuudatustele, mis mõjutavad kontrollikeskkondi;

10.1.3 P6 – Riskijuhtimise poliitika: lõimib audititulemused organisatsiooniülesesse riskihindamisse ja riskikäsitlusse;

10.1.4 P14 – Andmete säilitamise ja kõrvaldamise poliitika: reguleerib audititõendite, logide ja vastavuskirjete säilitamist;

10.1.5 P18 – Krüptograafiliste kontrollimeetmete poliitika: toetab tundlike auditiandmete turvalist säilitamist ja edastamist;

10.1.6 P26 – Kolmandate osapoolte ja tarnijate turbepoliitika: hõlmab auditeerimisõigusi, kindlustandvat dokumentatsiooni ja tarnijate vastavuse järelevalvet;

10.1.7 P30 – Intsidentidele reageerimise poliitika (P30): viib intsidentide käsitlemise protsesside auditid kooskõlla ISMS-i kontrollide tagamise eesmärkidega;

10.1.8 P32 – Talitluspidevuse ja katastroofitaaste poliitika: nõuab auditi tsüklite käigus talitluspidevuse testimise ja DRP vastavuse kontrollimist.

## 11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliste auditit ja pidevat vastavuse valideerimist käsitlevate standardite ning õigusnõuetega.

### 11.2 ISO/IEC 27001:

11.2.1 Punkt 9.2 – Siseaudit: nõuab ISMS-i regulaarseid riskipõhiseid auditeid, et hinnata tõhusust ja vastavust.

11.2.2 Punkt 9.3 – Juhtkonna ülevaatus: audititulemused tuleb sisendina arvesse võtta strateegilisel läbivaatamisel ja täiustamisel.

11.2.3 Punkt 10.1 – Mittevastavus ja parandusmeede: auditileiud tuleb käsitleda dokumenteeritud CAPA-protseduuride kaudu.

### 11.3 ISO/IEC 27002:2022 – Kontrollimeetmed 5.35–5.37:

11.3.1 Lisa A kontrollimeetmed 5.35–5.37: hõlmavad sõltumatut läbivaatamist, vastavust õiguslikele ja lepingulistele nõuetele ning auditilogimist.

11.3.2 Annavad rakendusjuhised auditi- ja vastavusprogrammide planeerimiseks, läbiviimiseks ja täiustamiseks.

### 11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontrollide hindamine: nõuab rakendatud turbekontrollide rutiinset läbivaatamist.

11.4.2 CA-5 – Tegevuskava ja verstapostid (POA&M): on kooskõlas auditileidude jälgimise ja kõrvaldamisega.

11.4.3 CA-7 – Pidev seire: toetab ennetavaid ja automatiseeritud vastavushindamisi.

### 11.5 EL GDPR (2016/679):

11.5.1 Artiklid 24 ja 32: nõuavad tõendeid turbekontrollide rakendamise ja tõhususe kohta asjakohaste juhtimisstruktuuride kaudu.

11.5.2 Artikkel 33: toetab vajadust kontrollitud auditijälgede järele rikkumistele reageerimisel ja neist teavitamisel.

### 11.6 EL NIS2 direktiiv (2022/2555):

11.6.1 Artikkel 21(2)(g): nõuab poliitikate ja protseduuride auditeerimist osana minimaalsetest küberturberiski juhtimise meetmetest.

11.6.2 Artikkel 27: riiklikud asutused võivad oluliste ja tähtsate üksuste puhul auditeid läbi viia või nende läbiviimist nõuda.

**11.7 EL DORA (2022/2554):**

11.7.1 Artikkel 10(2)(e): üksused peavad läbi viima IKT-riski juhtimise praktikate sise- ja välisauditeid.

11.7.2 Artikkel 25 – Auditinõuded: nõuab perioodilisi auditeid siseaudiitoritelt või sõltumatutelt välisaudiitoritelt koos regulatiivse nähtavusega.

**11.8 COBIT 2019:**

11.8.1 MEA01 – Tulemuslikkuse ja vastavuse seire, hindamine ja auditeerimine: tagab, et kontrollimeetmete tõhusus on kontrollitud ja juhtorganitele raporteeritud.

11.8.2 MEA03 – Vastavuse seire, hindamine ja auditeerimine: nõuab organisatsiooni praktikate kooskõla õiguslike, lepinguliste ja standardipõhiste nõuetega.