

Infoturbe poliitika

1. Üldsätted

Käesolev dokument kehtestab RMK infoturbe eesmärgid ja põhimõtted ning kirjeldab infoturbe halduse süsteemi (ISMS) juhtimise ja toimimise aluseid vastavalt ISO/IEC 27001:2022 standardile. Dokument loob ühtse raamistiku infoturbe strateegiliseks ja operatiivseks juhtimiseks RMK-s ning on aluseks infoturbealastele juhenditele ja protseduuridele.

1.1. Eesmärk

Dokumendi eesmärk on kehtestada RMK infoturbe juhtimise poliitika, mis loob aluse infoturbe planeerimiseks, rakendamiseks ja arendamiseks ning kirjeldab infoturbe juhtimise põhimõtteid arusaadavalt kõigile töötajatele ja juhtkonnale.

Dokument ei ole mõeldud tehniliste juhiste kogumikuna, vaid suunava ja selgitava alusdokumendina, millele tuginevad täpsemad juhendid ja töökorralduslikud juhised.

1.2. Staatus ja seos juhtimissüsteemiga

Dokument on kinnitatud RMK juhatuse poolt ning kuulub RMK üldise juhtimissüsteemi kesksete raamdokumentide hulka. Infoturbe juhtimist käsitletakse RMK-s lahutamatu osana organisatsiooni juhtimisest, olles seotud riskijuhtimise, kvaliteedijuhtimise ja protsessijuhtimisega. Infoturbe kaalutlused on osa juhtimisotsustest, arendusprojektidest ja igapäevasest töökorraldusest.

Infoturbe juhtimise poliitika on RMK infoturbe dokumentatsiooni hierarhias alusdokument. Kõik infoturbe valdkonda käsitlevad teemapoliitikad, juhendid ja töökorralduslikud dokumendid peavad olema käesoleva poliitikaga kooskõlas ning sellest lähtuma.

Infoturbe teemapoliitikaid ja juhendeid võivad kehtestada, muuta ja kehtetuks tunnistada vastava valdkonna eest vastutavad struktuuriüksuste juhid või dokumendi omanikud vastavalt RMK dokumendihalduse korrale. Juhatuse kinnitab infoturbe juhtimise poliitika ning vajaduse korral ka teatud valdkondlikud juhendid (nt [RMK riskide ja võimaluste haldamise juhend](#) jt), kuid ei pea kinnitama kõiki infoturbealaseid teemapoliitikaid ja juhendeid.

Kõik infoturbe ja andmekaitsega seotud teemapoliitikad, juhendid ja töökorralduslikud dokumendid, sõltumata nende kinnitamise tasemest, on käesoleva poliitika rakendamise osa ning töötajatele siduvad.

1.3. Mõisted ja lühendid

Käesolevas dokumendis kasutatavad mõisted ja lühendid on defineeritud "[Mõistete ja lühendite leksikonis](#)". Ühtse leksikoni kasutamine võimaldab hoida terminoloogia läbivalt järjepidevana kogu RMK dokumentatsioonis ning vältida mõistete dubleerimist või erinevat tõlgendamist.

2. Infoturbe eesmärgid ja põhimõtted

2.1. Infoturbe eesmärgid

Infoturbe juhtimise peamine eesmärk RMK-s on toetada organisatsiooni äri- ja tugiprotsesside sujuvat, katkematut ja usaldusväärset toimimist ning tagada andmete konfidentsiaalsus, terviklus ja käideldavus. Infoturbe eesmärgid on seatud viisil, mis võimaldab infoturvet juhtida ennetavalt ja tulevikku suunatult ning toetab selle pidevat parendamist kooskõlas ISO/IEC 27001:2022 standardi nõuetega.

Infoturbe eesmärkide saavutamiseks keskendutakse eelkõige järgmistele valdkondadele:

- RMK protsesside toimepidevuse ja töökindluse tagamine;
- infoturbe riskide ennetav vähendamine;
- tehnoloogilise võla ja aegunud lahendustest tulenevate riskide vähendamine;
- infoturbe küpsuse järkjärguline tõstmine;
- infoturbe integreerimine RMK strateegilisse ja operatiivsesse juhtimisse.

Infoturbe eesmärkide täitmist jälgitakse regulaarselt kehtestatud tulemusnäitajate (KPI-de) kaudu, mis kehtestatakse juhatuse otsusega. KPI-de tulemusi analüüsitakse infoturbe halduse süsteemi (ISMS) seire ja juhtkonna ülevaatuste käigus ning nende põhjal tehakse otsuseid infoturbe prioriteetide, ressursside ja parendustegevuste osas. Vajaduse korral korrigeeritakse eesmärgi ja meetmeid, et tagada nende vastavus RMK strateegilistele eesmärkidele ja muutunud riskikeskkonnale.

2.2. Infoturbe juhtimise põhimõtted

Infoturbe juhtimisel lähtub RMK riskipõhisest lähenemisest, mille kohaselt hinnatakse võimalikke ohte ja nende mõju ning rakendatakse turvameetmeid vastavalt riskide olulisusele. Meetmeid rakendatakse optimaalsel tasemel, tagades nende proportsionaalsuse, põhjendatuse ning kooskõla RMK tööprotsessidega.

Infoturbe meetmed peavad olema kooskõlas kehtivate õigusaktide ja lepinguliste kohustustega ning integreeritud igapäevastesse tööprotsessidesse. Infoturbe ei ole ainult reeglite kogum, vaid osa organisatsioonikultuurist, mille eest vastutavad nii juhid kui ka töötajad.

Infoturbe hõlmab lisaks infosüsteemidele ja andmetele ka füüsilist keskkonda, töövahendeid ning töötajate igapäevast käitumist. Seetõttu hõlmab infoturbe ka dokumentide ja andmekandjate nõuetekohast käitlemist, töökohtade ja ruumide turvalisust, ekraanide lukustamist ning pääsuõiguste, võtmete ja juurdepääsuvahendite vastutustundlikku haldamist.

3. Infoturbe kohaldumisaala

Infoturbe juhtimise poliitika kohaldub kõigile RMK äri- ja tugiprotsessidele ning hõlmab kõiki RMK töötajaid, infosüsteeme, infovarasid ja muid varasid sõltumata nende asukohast, vormist või tehnilisest lahendusest. Raamistik kehtib nii elektroonilisele kui ka paberkandjal teabele.

Samuti kohaldub infoturbe juhtimise raamistik välistele osapooltele ulatuses, mis tuleneb RMK ja partnerite vahelistest lepingutest, koostöösuhetest või õigusaktidest, sealhulgas olukordades, kus välised teenuseosutajad töötlevad RMK teavet või kasutavad RMK infosüsteeme.

4. Juhtkonna roll ja vastutus infoturbe tagamisel

RMK juhatus vastutab infoturbe juhtimise eest organisatsioonis ning kujundab infoturbe juhtimise üldised suunad ja ootused. Juhatus tagab, et infoturbe nõuded on arvesse võetud strateegilistes otsustes, ressursside planeerimisel ning tegevuste prioriseerimisel.

Juhtkonna roll ei piirdu üksnes dokumentide kinnitamisega, vaid hõlmab ka infoturbe eesmärkide seadmise, nende täitmise jälgimise ning vajaduse korral parenduste algatamise. Sellega luuakse organisatsioonis selge alus, et infoturbe on RMK juhtimise loomulik osa.

Kõik RMK töötajad vastutavad infoturbe nõuete järgimise eest oma tööülesannete täitmisel ning peavad tegutsema viisil, mis ei sea ohtu RMK teavet, infosüsteeme ega organisatsiooni mainet.

5. Infoturbe halduse süsteem (ISMS)

RMK infoturbe halduse kontseptsioon põhineb riskipõhisel juhtimisel ning on ellu viidud ISMS kaudu kooskõlas ISO/IEC 27001:2022 standardiga.

5.1. ISMS eesmärk

RMK ISMS eesmärk on tagada infoturbe juhtimise järjepidevus, läbipaistvus ja kontrollitavus. ISMS loob struktuuri, mille abil infoturbe eesmärged planeeritakse, rakendatakse, jälgitakse ja parendatakse süsteemselt ning dokumenteeritult.

ISMS on üles ehitatud vastavalt ISO/IEC 27001:2022 standardi nõuetele ning toetab RMK infoturbe juhtimise küpsuse järkjärgulist tõstmist.

5.2. ISMS toimimise põhimõtted

RMK loob, rakendab, hooldab ja täiustab ISMS-i pidevalt, lähtudes riskihindamise tulemustest, organisatsiooni arengust ja muutustest tegevuskeskkonnas. ISMS toimib tsüklilise juhtimismudelina, kus infoturbe meetmete planeerimine, rakendamine, seire ja parendamine moodustavad pideva protsessi.

6. Organisatsiooni kontekst ja huvipooled

Infoturbe juhtimisel arvestab RMK oma tegevuskonteksti, strateegilisi eesmärged ning sise- ja väliskeskkonna mõjusid. Infoturbe seisukohalt olulised huvipooled ning nende ootused ja nõuded on muuhulgas:

- **sisemised huvipooled:** RMK nõukogu, juhatus ja töötajad;
- **välised huvipooled:** järelevalveasutused (sh RIA), kliendid ja külastajad, koostöö- ja lepingupartnerid ning teised asutused ja teenuseosutajad, kelle infosüsteemidest RMK tegevus sõltub või kelle tegevus sõltub RMK infosüsteemidest.

Infoturbe juhtimine lähtub huvipoolte ootustest ja nõuetest, kohaldatavatest õigusaktidest, sealhulgas küberturvalisust ja andmekaitset reguleerivatest nõuetest, ning lepingulistest kohustustest.

7. Rollid ja vastutused infoturbe juhtimisel

Infoturbe juhtimine RMK-s eeldab selgelt määratletud rolle ja vastutust. Infoturbe juhtimises osalevad juhatus, infoturbejuht, infoturbe tööühm, protsessiomanikud, riskihalduse koordineerija, erinevad IT spetsialistid ning siseaudiitorid. Rollide ja vastutuse selge määratlemine aitab vältida dubleerimist ning tagab, et infoturbe küsimused on käsitletud õigel tasandil.

Infoturbe juhtimise eest RMK-s vastutavad:

- RMK juhatus vastutab infoturbe juhtimise üldise suuna eest, kinnitab infoturbe juhtimise poliitika ning tagab infoturbe integreerimise organisatsiooni juhtimissüsteemi.
- Infoturbejuht vastutab infoturbe halduse süsteemi (ISMS) eestvedamise, igapäevase toimimise, seire ja parendamise ning infoturbe juhtimise poliitika ja sellega seotud dokumentatsiooni ajakohasuse eest.
- Struktuuriüksuste juhid vastutavad selle eest, et nende vastutusvaldkonnas järgitakse infoturbe juhtimise poliitikat ning sellega seotud teemapoliitikaid ja juhendeid.
- Siseaudiitor vastutab ISMS-i perioodilise ja sõltumatu hindamis eest, et tagada turvameetmete vastavus õigusaktidele, standarditele ja asutuse eesmärkidele. Audit annab juhtkonnale objektiivse kinnituse ISMS toimivuse ja parendusvajaduste kohta.
- RMK töötajad vastutavad infoturbe nõuete järgimise eest oma tööülesannete täitmisel ning teabe ja infosüsteemide nõuetekohase kasutamise eest.
- Väliste teenuseosutajate ja koostööpartnerite infoturbealaste nõuete järgimise eest vastutab lepingut sõlmiv struktuuriüksus vastavalt lepingulistele kokkulepetele.

Muud infoturbe halduse süsteemi toimimiseks olulised rollid ja vastutused on täpsustatud käesolevas dokumendis ning asjakohastes teemapoliitikates, juhendites ja ametijuhendites.

Infoturbe juhtimise erinevate alamteemade, nt riskijuhtimine, infoturbeintsidentide käsitlemine, ligipääsu haldus, varade haldus jt, täpsemad rollid ja vastutused on määratud vastavates teemapoliitikates ja juhendites.

8. Riskide ja infovarade haldus

Infoturbe juhtimine RMK-s põhineb riskihaldusel ning on lahutamatu osa RMK üldisest riskihaldusest. Infoturbe riskide haldamine toimub kooskõlas „[RMK riskihalduse juhendiga](#)“, mille alusel infoturbe riskid tuvastatakse, hinnatakse, käsitletakse ja jälgitakse, et vähendada võimalike ohtude mõju RMK tegevusele.

Infovarade ja muude varade haldus toetab riskipõhist infoturbe rakendamist ning aitab suunata turvameetmeid eelkõige nendele varadele ja protsessidele, mille mõju RMK tegevusele on kõige suurem.

9. Intsidendid ja toimepidevus

Infoturbe ja andmekaitse intsidentide käsitlemine toimub vastavalt „[Infosüsteemidega seotud pöördumiste, intsidentide, muudatuste ja konfiguratsioonihalduse juhendile](#)“ ning selle lisadele. Eesmärk on ennetada intsidentide toimumist ning tagada, et nende esinemisel oleks organisatsioon valmis reageerima kiiresti ja koordineeritult.

Infoturbe või andmekaitsega seotud probleemide, kahtluste või ebatavaliste olukordade korral, sh näiteks tõrked infosüsteemides, arvutite ja mobiilsete

seadmetega, kasutajakontodega ja juurdepääsõiguste või andmete turvalisusega, **tuleb sellest viivitamata teavitada [IT-abi](#)**.

Toimepidevuse tagamiseks on määratletud kriitilised protsessid ja nende tööks vajalikud infosüsteemid, koostatud taasteplaanid, neid testitakse ning rakendatakse kriisihalduse põhimõtteid, et minimeerida häirete mõju RMK tegevusele.

10. Koolitus ja teadlikkus

RMK tagab infoturbealase teadlikkuse järjepideva tõstmise. Teadlikkuse suurendamine vähendab inimfaktorist tulenevaid riske ning toetab infoturbe meetmete tõhusat rakendamist.

Selleks rakendatakse kohustuslikku „[Infoturbe teadlikkuse arenguprogrammi](#)“, koolitatakse sihipäraselt võtmerollides töötavaid isikuid ning kaasatakse juhte infoturbe väärtuste ja heade praktikate edendamisse. Vajaduse korral viiakse läbi täiendavaid koolitusi ja teavitustegevusi, lähtudes rollipõhistest vajadustest ja tuvastatud riskidest.

Infoturbealase teadlikkuse ja kultuuri kujundamine on osa RMK juhtimisest ning selle eest vastutavad juhatus ja struktuuriüksuste juhid oma vastutusvaldkonnas. Juhid tagavad, et infoturbe põhimõtted on töötajatele arusaadavad, neid rakendatakse igapäevatöös ning infoturbe teemad on integreeritud töö- ja otsustusprotsessidesse. Teadlikkuse tõstmine toimub järjepidevalt koolituste, kommunikatsiooni ja praktiliste juhiste kaudu ning seda toetatakse infoturbe halduse süsteemi raames.

11. Seire, ülevaatused ja parendamine

ISMS toimivust seiratakse pidevalt, kasutades asjakohaseid mõõdikuid ja hindamismeetodeid. Seire tulemused annavad sisendi juhtkonna ülevaatuks ning aitavad hinnata infoturbe meetmete tõhusust ning nende vastavust seatud eesmärkidele.

Infoturbe seire, auditite ja ülevaatuste tulemused koondatakse ning analüüsitakse süsteemselt, et tuvastada kõrvalekaldeid, nõrkusi ja parendusvõimalusi. Analüüsi tulemused esitatakse juhtkonnale, kes määrab parendustegevuste prioriteedid ning otsustab nende elluviimise. Parendustegevused planeeritakse ja viiakse ellu ning nende mõju hinnatakse järjepidevalt, tagades infoturbe halduse süsteemi pideva täiustamise.

Juhtkonna ülevaatused viiakse läbi regulaarselt, vähemalt kord aastas, lähtudes seire, auditite ja muude tagasisideallikate tulemustest.

12. Auditid ja mittevastavuste haldus

Infoturbe juhtimise vastavust hinnatakse siseauditite ning sõltumatute sertifitseerimisauditite kaudu. Auditid annavad juhtkonnale kindluse, et infoturbe juhtimine toimib kavandatud viisil.

Tuvastatud mittevastavused registreeritakse Jira projektis „ISO27001“, neid analüüsitakse ja käsitletakse vastavalt kehtestatud korrale, et vältida korduvaid probleeme ning toetada infoturbe pidevat parendamist.

13. Dokumentatsiooni haldus ja seosed

Infoturbe dokumentatsiooni hallatakse elektrooniliselt RMK dokumendihaldussüsteemis (DHS), samuti teistes RMK kasutatavates keskkondades, sh Microsoft 365 ja Jira, vastavalt „[Infoturbe dokumentatsiooni haldamise](#)“ põhimõtetele.

RMK-s on infoturbe juhtimise poliitika elluviimiseks ja toetamiseks kehtestatud teemapoliitikad, juhendid ja töökorralduslikud dokumendid, mis käsitlevad ISO/IEC 27001:2022 standardis nimetatud infoturbe valdkondi.

Infoturbe ja andmekaitsega seotud teemapoliitikad, täpsemad nõuded ja töökorralduslikud juhised on koondatud Siseveebis [Infoturbe käsiraamatusse](#) ja [Andmekaitse käsiraamatusse](#), mis on töötajatele kättesaadavad vastavalt kehtestatud juurdepääsuõigustele. Töötajad peavad oma tööülesannete täitmisel lähtuma nendes käsiraamatutes toodud juhistest ja nõuetest.

Dokumente vaadatakse üle regulaarselt ning need ajakohastatakse vastavalt organisatsiooni, õigusruumi ja tehnilise keskkonna muutustele.