SISEMINISTEERIUM

KÄSKKIRI

13.09.2018 nr 1-5/99

Siseministeeriumi infoturbepoliitika

Käskkiri kehtestatakse Vabariigi Valitsuse 31. mai 2012. a määruse nr 39 „Siseministeeriumi põhimäärus“ § 23 lõike 2 punkti 2 ja Vabariigi Valitsuse 15. märtsi 2012. a määruse nr 26 „Infoturbe juhtimise süsteem” § 3 punkti 1 alusel.

1. Üldsätted

1.1. Infoturbepoliitika kehtestamise eesmärk on reguleerida infoturbe valdkonda Siseministeeriumis (edaspidi *ministeerium*) ning kirjeldada organisatsiooni üldist lähenemisviisi infoturbe tagamisel.
1.2. Infoturbepoliitika määrab ministeeriumi infoturbe eesmärgid, infoturbe juhtimise üldpõhimõtted ning turvaintsidentide käitlemise.
1.3. Infoturbepoliitikaga on kohustatud tutvuma kõik ministeeriumi ametnikud ja töötajad (edaspidi teenistuja) ning isikud, kellele on loodud ministeeriumi kasutajakonto või omavad juurdepääsu infosüsteemidele.
1.4. Ministeeriumi tõhusaks ja toimivaks igapäevategevuseks on tähtsad infovarad, mida tuleb kasutada ainult selleks määratud otstarbel ja millele ministeerium annab juurdepääsu üksnes teadmisvajaduse alusel.
1.5. Ministeeriumis koordineerib infoturbe haldamise ja rakendamisega seonduvat tegevust infoturbejuht, kes juhindub infoturbe valdkonna kohustuslikest nõuetest, üldtunnustatud standarditest ja hea tava soovitustest.
1.6. Infoturbepoliitika kujundamisel ja rakendamisel infoturbejuht lähtub Euroopa Parlamendi ja nõukogu määrusest 2016/679 (EL), küberturvalisuse seadusest, riigisaladuse ja salastatud välisteabe seadusest, Vabariigi Valitsuse 15. märtsi 2012. a määruses nr 26 „Infoturbe juhtimise süsteem” ja Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ ette nähtud nõuetest ja muudest valdkonda reguleerivatest õigusaktidest.

2. Terminid

2.1. Infoturve ehk andmekaitse tähendab andmete kolme põhiomaduse – käideldavuse, tervikluse ja konfidentsiaalsuse – tagamist.
2.2. Andmed on informatsiooni taastõlgendatav esitus varem kokkulepitud kujul ja kandjal, näiteks paberdokumendina, digisalvestisena magnetkettal, mikrofilmina, fotona jts.
2.3. Informatsioon ehk teave on igasugune teadmine, mis puudutab fakte, sündmusi, asju, protsesse või ideid, ja millel on teatud kontekstis eritähendus.
2.4. Infovara moodustavad ministeeriumi valduses olevad andmed ja nende nõuetekohast töötlemist tagavad info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) vahendid, milleks muuhulgas on riist- ja tarkvara, andmesideseadmed ning IKT taristu.
2.5. Intsident on kõrvalekalle teenuse kokkulepitud toimimisest.
2.6. Turvaintsident on intsidendi alaliik, milleks on sündmus või sündmused, millega kaasneb andmete, sealhulgas isikuandmete või muude infovarade käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib märkimisväärne oht andmete käideldavuse, tervikluse või konfidentsiaalsuse kao tekkeks.
2.7. Kontrolljälg ehk logi (edaspidi *logi*) salvestatakse intsidendi jälitatavuse tagamiseks ning infovarade haldamise ja kasutamisega seotud toimingute tegemise kohta. Ministeeriumi kontrolljälgi salvestab ja säilitab Siseministeeriumi infotehnoloogia- ja arenduskeskus (edaspidi *SMIT*) ja kontrolljälgedega on õigus tutvuda ministeeriumi infoturbejuhil.
2.8. Turvaklassiks loetakse Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ (edaspidi *ISKE juhend*) alusel määratud infovara turvaklassi.

3. Infoturbe eesmärgid

3.1. Infoturbe eesmärgid on järgmised:
3.1.1. tagada stabiilne, turvaline ja töökindel töökeskkond ja säilitada infosüsteemide talitlusvõime ministeeriumi igapäevase asjaajamise ja infovahetuse korraldamisel;
3.1.2. tagada ministeeriumile töötlemiseks või hoidmiseks antud andmete käideldavus, konfidentsiaalsus ja terviklus;
3.1.3. kavandada, arendada ja pidada infosüsteeme ja andmekogusid õigusaktidest tulenevate infoturbenõuete kohaselt;
3.2. Infoturbe eesmärkide saavutamiseks tagatakse teenustaseme kokkulepetega infovaradele järgmised kolm põhiomadust:
3.2.1. käideldavus – andmete õigeaegne ja mugav kättesaadavus ning nende kasutatavus nii tava- kui ka kriisiolukorras ning infosüsteemide talituspidevus;
3.2.2. terviklus – töödeldavad andmed on usaldatavad ja andmete tõepärasust kontrollitakse regulaarselt;
3.2.3. konfidentsiaalsus – konfidentsiaalse teabe ja konfidentsiaalsete andmete kaitse vastab asjakohastele õigusaktides sätestatud nõuetele ning juurdepääs andmetele antakse üksnes teadmisvajaduse korral.

4. Infoturbejuht

4.1 Ministeeriumi infoturbejuht (edaspidi *infoturbejuht*) koordineerib ministeeriumis infoturbe valdkonna tööd ja vastutab infoturbega seotud ülesannete täitmise eest. Infoturbejuht allub vahetult kantslerile.
4.2. Infoturbejuhi põhiülesanded on järgmised:
4.2.1. korraldab infoturvet reguleerivate ministeeriumi-siseste kordade ja juhiste väljatöötamise, tagab nende ajakohastamise ning kontrollib nende täitmist;

4.2.2. teavitab punktis 1.3 nimetatud isikuid infoturbereeglitest, nõustab neid organisatoorsete ja füüsiliste infoturbemeetmete rakendamisel ning korraldab neile regulaarselt infoturbekoolitusi;
4.2.3. teavitab turvaintsidendist viivitamata kantslerit, infohaldusosakonna juhatajat ja otsustab vajaduse teavitada SMIT-i infoturbejuhti või Riigi Infosüsteemi Ametit;
4.2.4 koostöös Politsei- ja Piirivalveameti ja SMIT-iga töötab välja infoturbealaseid teste ja kooskõlastatult kantsleriga viib ministeeriumis ette teatamata läbi infoturbealast testimist;
4.2.5. teeb turvaintsidentide osas ettepanekuid teenistusliku järelevalve algatamiseks siseauditi osakonnale.

5. Turvaintsidendi lahendamine

5.1. Turvaintsidendi lahendamine toimub infoturbejuhi või kantsleri poolt selleks määratud teenistuja koordineerimisel.
5.2. Turvaintsidendist või selle ohust peab punktis 1.3 nimetatud isik viivitamata teavitama infoturbejuhti.
5.3. Turvaintsidendi avastaja peab tegema kõik endast oleneva, et turvaintsident jääks võimalikult väikeseks ja ei laieneks.
5.4. Isikuandmetega seotud rikkumisest teavitab ministeeriumi infoturbejuht ministeeriumi andmekaitseametnikku, kes asjakohasel viisil teavitab sellest Andmekaitse Inspektsiooni ja otsustab vajaduse teavitada andmesubjekti.
5.5. Turvaintsidendi lahendamisel jälgib infoturbejuht selle lahendamise kulgu, teeb vajaduse korral ettepanekuid turvaintsidendi paremaks lahendamiseks, koostab pärast turvaintsidendi lahendamist aruande ning analüüsib turbeintsidendi põhjuseid ja lahendamise käiku. Kui turvaintsidendi käigus on rikutud isikuandmeid, kaasab infoturbejuht turvaintsidendi lahendamisse ministeeriumi andmekaitseametniku.
5.6. Infoturbejuht on kohustatud täitma turvaintsidendi raporti (edaspidi *raport*) ja pidama raportite üle arvestust. Raportid edastatakse ministeeriumi kantslerile, infohaldusosakonna juhatajale ja vajaduse korral ka kantsleri määratud teenistujale.
5.7. Andmekaitseametnik dokumenteerib isikuandmetega seotud rikkumise korral kõik isikuandmetega seotud rikkumised, sealhulgas selle rikkumise asjaolud, mõju ja kasutusele võetud parandusmeetmed.
5.8. Turvaintsidendi avastamise üks eeldusi on turvaintsidendi jälitatavuse toimivus. Selleks, et tagada turvaintsidendi jälitatavus, salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud toimingute tegemise kohta kontrolljälgi ehk logisid. Toimingute liik, mille tegemise kohta kontrolljälgi salvestatakse ja säilitatakse, samuti kontrolljälgede säilitamise tähtaeg kehtestatakse vastavalt õigusaktides sätestatud nõuete kohaselt ning infovaradele määratud turvaklassi ja sellele vastavate ISKE rakendusjuhendis sisalduvate turvameetmete järgi.
5.9. Turvaintsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse ja seda analüüsitakse infoturbejuhi poolt, et selliste intsidentide aset leidmist edaspidi vältida ja otsustada vajaduse üle võtta kasutusele uusi turvameetmeid.

6. Vastutus

6.1. Punktis 1.3 nimetatud isikud peavad juhinduma infoturbepoliitika eesmärkidest, infoturvet reguleerivatest juhistest ja järgima isikuandmete kaitse nõudeid, kui täidavad teenistus- ja tööülesandeid ministeeriumis kohapeal või kaugtöö paigas.

6.2. Punktis 1.3 nimetatud isikud vastutavad juhul kui:
6.2.1. ei järgi infoturbepoliitika eesmärke ning ei pea kinni infoturvet reguleerivatest juhistest ja isikuandmete kaitse nõuetest,
6.2.2. ei teavita viivitamatult turvaintsidendi avastamise korral infoturbejuhti või
6.2.3. turvaintsidendi avastamise korral ei tee endast olenevat, et takistada turvaintsidendi laienemist.

7. Rakendussäte

7.1. Tunnistan kehtetuks kantsleri 1. oktoobri. 2014. a käskkirja nr 1-5/174 „Siseministeeriumi infoturbe kord“.

(allkirjastatud digitaalselt)

Lauri Lugna
kantsler

Lisa 1 turvaintsidendist teavitamise vorm.