Seletuskiri „Siseministeeriumi infoturbepoliitika“ eelnõu juurde

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõu on välja töötatud eesmärgiga kehtestada Siseministeeriumi infoturbepoliitika, mida on kohustatud järgima kõik ministeeriumi teenistujad ning isikud, kellele on loodud kasutajakonto või omavad juurdepääsu infosüsteemidele. Infoturbepoliitikaga tagatakse üldised infoturbe eesmärgid, samuti kehtestatakse infoturbejuhi põhiülesanded ja reguleeritakse turvaintsidentide käsitlemise üldised alused ning tagatakse intsidendi jälitatavuse toimimine. Samuti on käskkirjas kindlaks määratud teenistujate ja kasutajakontot omavate isikute või juurdepääsu infosüsteemidele omavate isikute vastutus.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Siseministeeriumi infohaldusosakonna nõunik Martin Sepp (Martin.Sepp@siseministeerium.ee, tel 612 5249) ja Siseministeeriumi õigusosakonna nõunik Kertu Nurmsalu (kertu.nurmsalu@siseministeerium.ee, tel 612 5084). Eelnõu ja seletuskirja on keeleliselt toimetanud Siseministeeriumi õigusosakonna keeletoimetaja Airi Kapanen (airi.kapanen@siseministeerium.ee, tel 612 5241).

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb seitsmest peatükist:
1. Üldsätted;
2. Terminid;
3. Infoturbe eesmärgid;
4. Infoturbejuht;
5.Turvaintsidendi lahendamine;
6. Vastutus;
7. Rakendussäte.

Eelnõuga kavandatav peatükk 1. Üldsätted

Siseministeeriumi (edaspidi *ministeerium*) infoturbepoliitikaga määratakse kindlaks ministeeriumi infoturbe eesmärgid, infoturbe juhtimise üldpõhimõtted ja infoturbe strateegia üldalused. Ministeeriumi infoturbepoliitika eesmärk on kirjeldada organisatsiooni üldist lähenemisviisi, et tagada infoturve samal ajal ministeeriumile pandud tööülesannete täitmisega. Käskkirjas pööratakse tähelepanu infoturbe haldamise ja rakendamisega seotud tegevusele, nagu juurdepääs teadmisvajaduse alusel, infovarade turvaline käitlemine ja tegutsemine turvaintsidentide korral. Samuti on täpselt kindlaks määratud infoturbejuhi roll ja see, kuidas on infoturbeintsidentide korral tagatud intsidendi jälitatavuse toimimine.

Käskkirjaga on kohustatud tutvuma kõik ministeeriumi ametnikud ja töötajad, keda käskkirjas nimetatakse teenistujateks, aga samuti ka isikud, kes ei ole teenistujad, kuid kellele on loodud ministeeriumi kasutajakonto (edaspidi ka *käskkirjas nimetatud isikud*). Eelkõige on sellisteks isikuteks praktikandid või võlaõigusliku lepingu alusel teenust osutavad isikud, neile võimaldatakse loodud kasutajakonto kaudu ligipääs ministeeriumi infosüsteemidele, kuid neil ei ole püsivat tööalast suhet ministeeriumiga. Välistatud ei ole, et infosüsteemidele omavad juurdepääsu ka isikud, kellel ei ole ministeeriumi kasutajakontot, näiteks juurdepääs andmekogule, mille vastutav töötleja on ministeerium.

Eelnõuga kavandatav peatükk 2. Terminid

Eelnõu teises peatükis on määratletud infoturbe terminid, nagu „infoturve“, „andmed“, „informatsioon“, „infovarad“, „intsident“, „turvaintsident“; „kontrolljälg“ ja „turvaklass“.

Terminiloetelu koostati järgmiste dokumentide alusel:

1. Vabariigi Valitsuse 15. märtsi 2012. a määruse nr 26 „Infoturbe juhtimise süsteem” § 2 ja
2. Siseministeeriumi kantsleri 1. oktoobri 2014 käskkirja nr 1-5/174-„Siseministeeriumi infoturbe kord“ punkt 2.

Ühtsed terminid võimaldavad käskkirjas nimetatud isikutel paremini mõista ja selgitada Siseministeeriumi infoturbepoliitikat ning infoturbepoliitikast tulenevaid nõudeid.

Eelnõuga kavandatav peatükk 3. Infoturbe eesmärgid

Infoturbe eesmärk on tagada stabiilne, turvaline ja töökindel töökeskkond ja säilitada infosüsteemide talitlusvõime ministeeriumi igapäevase asjaajamise ja infovahetuse korraldamisel ja samuti tagada ministeeriumile töötlemiseks või hoidmiseks antud andmete käideldavus, konfidentsiaalsus ja terviklus. Infoturve on organisatsiooni kollektiivne tegevus ja kõikide teenistujate ja kasutajakontot või ministeeriumi infosüsteemidele ligipääsu omavate isikute kohustus. Infoturbega seotud riskid jagunevad järgmiselt: organisatsioonilised nõrkused; personaliga seotud nõrkused; infrastruktuuri nõrkused ja tehnoloogia nõrkused. Eeltoodu kohaselt peab riskidega toimetulekuks iga käskkirjas nimetatud isik teadma, milles seisneb tema panus infoturbesse. Samuti on infoturbe toimimiseks vaja peale eesmärkide teadvustamise määrata käskkirjaga ministeeriumis rollid ja vastutus infoturbe valdkonnas.

Infoturbe eesmärkide saavutamiseks tuleb tagada infovaradele kohalduvat kolm peamist infoturbe põhiomadust, sõltumata sellest, millist etalonturbe süsteemi (ISKE, ISO/IEC 27001, ISO/IEC 27002, CIS Critical SecurityControls, COBIT 5, IASME Cyber Essentials Scheme või NIST SpecialPublication 800-53) rakendatakse.

Ministeerium rakendab praegu ISKE etalonturbe süsteemi. Seega peavad olema tagatud kolm infoturbe põhiomadust:
1) käideldavus – kuna ministeerium kasutab infosüsteeme oma igapäevaste tööülesannete täitmiseks;
2) terviklus – töödeldavad andmed peavad olema usaldatavad ja andmete tõepärasust tuleb regulaarselt kontrollida;
3) konfidentsiaalsus – konfidentsiaalsete teabe ja andmete kaitse peab olema selgelt kindlaks määratud ja vastama asjakohastele seadusenõuetele. Juurdepääs informatsioonile antakse ainult tõendatud teadmisvajaduse alusel.

Põhiomaduste tagamiseks sõlmitakse teenustaseme kokkulepped tulenevalt kantsleri 19. juuli 2018. a käskkirjast nr 1-5/88 „Siseministeeriumi info- ja kommunikatsioonitehnoloogia teenuste osutamise põhimõtted“

Eelnõuga kavandatav peatükk 4. Infoturbejuht

Vabariigi Valitsuse 15. märtsi 2012. a määruse nr 26 „Infoturbe juhtimise süsteem” § 3 punkti 3 kohaselt tuleb asutuse juhil luua infoturbejuhi ametikoht ning määrata infoturbejuht või kokkuleppel teise asutuse juhiga täidab neid ülesandeid teise asutuse infoturbejuht või asutuseväline teenuseosutaja (edaspidi *infoturbejuht*). Infoturbejuht allub infoturbeküsimustes vahetult kantslerile. Samuti annab eelnimetaud määruse § 4 lõike 4 punkti 4 kohaselt infoturbejuht oma tegevusest aru kantslerile ning koostab vähemalt kord aastas infoturbe üldraporti.

Infoturbejuht korraldab ministeeriumis tegevust infoturbe valdkonnas ja vastutab infoturbega seotud ülesannete täitmise eest. Infoturbejuht nõustab infoturbeküsimustes ministeeriumi teenistujaid ning isikud, kellele on loodud ministeeriumi kasutajakonto või omavad juurdepääsu infosüsteemidele. Infoturbejuht korraldab infoturvet reguleerivate poliitikate, standardite kujundamist ning kordade ja juhiste väljatöötamist ja kontrollib nende täitmist, infoturbemeetmete rakendamise tõhusust ning sellekohaste teavituste või raportite koostamist. Samuti korraldab infoturbejuht regulaarselt infoturbekoolitusi ning viib läbi ette teatamata infoturbe testimisi. Ette teatamata infoturbe testimistega kontrollitakse teenistujate ja käskkirjas nimetatud isikute hoolsuskohustust ja teadmisi infoturbe reeglite täitmisel.

Infoturbejuht teavitab viivitamata kantslerit ja infohaldusosakonna juhatajat turvaintsidendist ning olenevalt turvaintsidendist, võttes arvesse selle levikut, kaasneda võivaid riske jmt otsustab, kas sellest on vaja teavitada ka SMITi või Riigi Infosüsteemi Ametit.

Eelnõuga kavandatav peatükk 5. Turvaintsidendi lahendamine

Peatükis „Turvaintsidendi lahendamine“ määratakse käskkirjas nimetatud isikute ning infoturbejuhi tegevus turvaintsidendi lahendamisel. Isik, kes avastab turvaintsidendi, on kohustatud esimesel võimalusel ehk viivitamata teavitama sellest infoturbejuhti ning võtma meetmed, et turvaintsident ei laieneks ja selle mõju oleks võimalikult väike.

Infoturbejuht jälgib turvaintsidendi lahendamise kulgu, teeb vajaduse korral ettepanekuid turvaintsidendi paremaks lahendamiseks ja analüüsib turvaintsidendi tekkepõhjuseid ja lahendamise käiku ning vajaduse korral teavitab turvaintsidentidest pädevaid asutusi. Turvaintsidendi põhjuste analüüsimine aitab edaspidi vältida sarnaseid võimalikke turvaintsidente. Samuti on infoturbejuht kohustatud täitma turvaintsidendi raporti ja pidama nende üle arvestust. Infoturbejuht teavitab isikuandmetega seotud rikkumisest ministeeriumi andmekaitseametnikku, kes Euroopa Parlamendi ja nõukogu määruse 2016/679 artiklite 33 ja 34 kohaselt teavitab Andmekaitse Inspektsiooni ja otsustab vajaduse teavitada ka andmesubjekti.

Turvaintsidentide avastamiseks ja selle jälitatavuse tagamiseks salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud toimingute tegemise kohta kontrollijälg ehk logisid. Kontrolljälgedel on tõenduslik väärtus ning hilisemas järelevalvemenetluses on võimalik kontrolljälgi kasutada tõenditena intsidendi avastamiseks ja intsidendi põhjuste

väljaselgitamiseks, samuti selleks, et võtta vastutusele turvaintsidendi eest vastutavad isikud või organisatsioonid. Kontrolljäljed sarnaseid turvaintsidente ennetada ja ära tunda ning võtta ennetusmeetmed. Kontrolljälgede salvestamise kohustus on Siseministeeriumi infotehnoloogia- ja arenduskeskusel, kuna nemad vastutavad ministeeriumi IKT-taristu toimimise eest.

Eelnõuga kavandatav peatükk 6. Vastutus

Käskkirjas on kindlaks määratud teenistujate vastutus. Lähtudes käskkirjast on ministeeriumi teenistujad kohustatud täitma infoturbejuhiseid ja järgima isikuandmete kaitse nõudeid. Teenistujad vastutavad nende rakendamise eest oma teenistuskohal teenistus- ja tööülesannete täitmisel, kuid ka siis, kui täidavad teenistus- või tööülesandeid ministeeriumist väljaspool.

Vastutuse alustena on käskkirjas toodud, et käskkirjas nimetatud isikud peavad oma ülesannete täitmisel juhinduma infoturbejuhisetest ja järgima isikuandmete kaitse nõudeid, seda niioma teenistuskohal teenistus- ja tööülesannete täitmisel, kuid ka siis, kui täidavad teenistus- või tööülesandeid ministeeriumist väljaspool.

Samuti vastutavad käskkirjas nimetatud isikud oma tegevuse või tegevusetusega põhjustatud kahju eest distsiplinaar-, väärteo- või kriminaalkorras. Vastavad alused on toodud avaliku teenistuse seaduses, karistusseadustikus või vastavat väärteokoosseisu sisaldavas eriseaduses ning seetõttu neid aluseid käesolevas käskkirjas toodud ei ole

3. Käskkirja mõju

Käskkirja jõustamise tulemusel on kindlaks määratud ministeeriumi infoturbe eesmärgid ja infoturbe juhtimise üldpõhimõtted ning infoturbe strateegia üldalused. Lähtudes Vabariigi Valitsuse 15. märtsi 2012. a määrusest nr 26 „Infoturbe juhtimise süsteem" võetakse kasutusele ühtsed infoturbeterminid, mis aitavad täpselt sisustada ja paremini selgitada ministeeriumi infoturbepoliitikat.

Ministeeriumi infoturbepoliitikat hakkab koordineerima infoturbejuht, kes vastutab infoturbega seotud ülesannete täitmise eest. Samuti reguleeritakse käskkirjaga infoturbeintsidentide lahendamine, infoturbeintsidentide jälitatavuse toimivus (ehk kontrollijälgede salvestamine), paraneb infoturbeintsidentide dokumenteerimine ja tekib kohustus sellest raporteerida. Infoturbeintsidentide dokumenteerimine võimaldab turbeintsidente analüüsida, et edaspidi nende aset leidmist vältida, nende analüüsimine aga võimaldab parendada ministeeriumi infoturbemeetmeid.

Kui infoturbeintsidendiga on kaasnenud isikuandme leke või oht isikuandmetele, kaasab infoturbejuht turvaintsidendi lahendamisse ministeeriumi andmekaitseametniku.

Käskkirja rakendumisel paraneb ministeeriumis teenistujate ja nende isikute, kellele on tehtud kasutakjakonto või omavad juurdepääsu infosüsteemidele infoturbeteadlikkus ja sellel on positiivne mõju ministeeriumi infoturbevaldkonnale.

4. Rakendussäte

Eelnõuga on kavandatud kehtetuks tunnistada kantsleri 1. oktoobri. 2014. a käskkirja nr 1- 5/174 „Siseministeeriumi infoturbe kord". Eelnõuga võetakse üle nimetatud käskkirjas

kasutusel oleva terminid, kuid vastutus ja rollid, infoturbejuhi ülesanded ning turvaintsidentide käsitlemine on eelnõus täpsemalt reguleeritud.

5. Käskkirja jõustumine

Käskkiri jõustub üldises korras.