# 5 ISKE RAKENDAMINE

ISKE rakendamisel kohalikus omavalitsuses tuleb nagu ka kõigis teistes asutustes lähtuda ISKE rakendusjuhendi metoodikast, läbides kõik 10 sammu. Siinses aruandes oleme erilist tähelepanu pööranud eelkõige alginfo kogumisele, millele kogu ISKE rakendamine tugineb, kuid kirjeldatud on ka kõik muud tegevused. ISKE viimane versioon 5.00 on juba tänu olulistele tõlketäiendustele piisava põhjalikkusega selgitanud ISKE üksikmeetmeid ning me ei pea vajalikuks ISKE juhiseid otse aruandesse ümber kopeerida, samuti pole otstarbekas neist lühivariante tekitada. Iga ISKEt rakendav organisatsioon on kohustatud kohapeal vajalikud ISKE meetmed ise läbi töötama. Seega lähtumegi eelkõige varasemast kogemusest tulenevalt probleemist – kuidas leida õiged ja vajalikud meetmed ja alustada nende rakendamisega.

Nagu igasuguse infoturbehaldussüsteemi rakendamisel on esimene kõige suurem probleem motivatsiooni ja huvi leidmine nii projekti meeskonnas kui kõigil KOViga seotud teenistujatel. Infoturve peab olema igapäevase töö loomulik osa, mis tagab KOVi tegevuste talituspidevuse, seadustele vastavuse ja tõrgeteta töö. Infoturve ei tohi olla eesmärk omaette, vaid peab lähtuma organisatsiooni eesmärkidest. Kuna täna me kasutame oma igapäeva tööd tehes infotehnoloogilisi vahendeid, mängib infoturbe tagamises olulist rolli KOVi kogu infosüsteem. Ükski süsteem ei toimi turvaliselt, kui selle kasutajad pole piisavalt turvateadlikud ja motiveeritud turvaliselt käituma. ISKE edukaks rakendamiseks tuleb paralleelselt realiseerida nii organisatsioonilised, füüsilised kui infotehnilised turvameetmed, neid plaanida, rakendada, seirata ja vajadusel täiendada ning muuta.

ISKE inventuuri läbiviimisel on soovitav kasutada juba olemasolevaid infovarade loendeid, neid täiendades vastavalt järgnevates jaotistes kirjeldatule. Abimaterjalina võib kasutada ka KOVi pilootprojekti tabeleid (http://www.ria.ee/29943), kuid tuleb arvestada, et pilootprojekti vastavad tööd viidi läbi 2008. aasta algul, mil kehtiv oli ISKE versioon 3.00, samuti on vahepeal muutunud ka mõningad nõuded seadusandluses (IKS, AvTS jms) ja kuna tegu on infoturbega, siis on näidismaterjali oluliselt kärbitud.

ISKE rakendamise kümme sammu (ISKE rakendusjuhendi punkt 1.5.1):

1. Asutuse IT eest vastutav töötaja koostöös ISKE koordinaatoriga ja asutuse juhtkonnaga viib läbi infovarade inventuuri ja spetsifitseerimise.
2. Iga andmekogu andmete omanik määrab koostöös ISKE koordinaatori ja infoturbe spetsialistiga andmekogule turvaklassi ning märgib turvaklassid infovarade spetsifikatsioonidesse. Mitte-siseseks kasutamiseks mõeldud andmekogude (nt e-post, varundus) puhul tuleb edastada turvaklass RIHAsse https://riha.eesti.ee/ kaudu.
3. IT eest vastutav töötaja koos infoturbe spetsialistiga määrab muude infovarade turvaklassi ning märgib turvaklassid infovarade spetsifikatsioonidesse.
4. Infoturbe spetsialist määrab kõikide turvaklassiga infovarade vajaliku turbeastme ja märgib turbeastmed infovarade spetsifikatsioonidesse.

5. Kui kõrgeimaks vajalikuks turbeastmeks osutus M või H, otsustab juhtkonna esindaja koos IT eest vastutava töötaja ja infoturbe spetsialistiga, kas rakendada kogu asutuses üks turbeaste või jaotada asutus eri turbeastmetega tsoonideks. Viimasel juhul kavandavad nad tsoonid ja selliste tsoonide loomiseks vajalikud muudatused. Kui turvaastmete määramisel ei ilmnenud vajadust turbeastet L ületavaks turbeks, rakendatakse aste L kogu asutuse ulatuses.
6. Infoturbe spetsialist vaatab läbi tüüpmoodulite kataloogi B, võrdleb seda infovarade spetsifikatsioonidega ja märgib spetsifikatsioonidesse tüüpmoodulite tähised. Kui tüüpmoodulite kataloogi läbivaatusel ilmneb veel spetsifitseerimata varasid, spetsifitseerib ta need varad töö selles järgus. Tüüpmoodulid, millele vastavaid varasid asutuses ei ole, jäetakse arvestamata; see nõue ei puuduta organisatsioonilisi varasid, mis kuuluvad moodulirühma B 1.
7. Infoturbe spetsialist koostab kõrgeimast määratud turbeastmest lähtudes turbehalduse meetmete loetelu, leides need meetmed mooduli B 1.0 turvaspetsifikatsiooni põhjal turvameetmete kataloogist M ja turbeastme H korral ka kataloogist H.
8. Infoturbe spetsialist koos juhtkonna esindaja ja asutuse IT eest vastutava töötajaga koostab plaani infoturbe halduse (moodul B 1.0) meetmete rakendamiseks, seejärel määrab muude infovarade turbe rakendamise prioriteedid ja turbe rakendamise plaani, arvestades ka meetmete rakendamise maksumuse ning ajalise kestvuse prognoose. Infoturbe halduse kavandamisel võib lisaks etalonmeetmete juhistele abivahendina kasutada ka standardites EVS-ISO/IEC TR 13335 ja EVSISO/IEC 27002 antud juhiseid.
9. Infoturbe spetsialist korraldab plaani täitmise, koostades turvameetmete loetelud tüüpmoodulite turvaspetsifikatsioonide ja turvameetmete kataloogide põhjal, juhindudes turbehalduse meetmetest ja kaasates töösse asjakohaseid töötajaid ja informeerides regulaarselt juhtkonda.
10. Pärast iga infovara turvameetmete evitamist kontrollib infoturbespetsialist vastava tüüpmooduli turvaspetsifikatsiooni ja ohtude kataloogi G alusel tegelikku turvaolukorda, arvestades tegelikke ohte konkreetses olukorras. Kui ilmneb mingeid ohte, mida tüüpmooduli turvaspetsifikatsioon ei arvesta, kontrollib ta rakendatud turvameetmete piisavust tegelikes tingimustes ning rakendab vajaduse korral täiendavaid turvameetmeid.

## 5.1 SAMMUD 1–4: INFOVARADE INVENTUUR JA SPETSIFITSEERIMINE

### 5.1.1 ISKE rakendamise töörühma loomine

ISKE rakendamise projekti õnnestumiseks tuleb luua töögrupp, milles oleks kaetud järgmised rollid (võivad mõnikord kohati kattuda):

- ISKE rakendamise **koordinaator** – projektijuht. Soovitavalt asutuse oma töötaja. Välistatud pole, et tegu on spetsiaalselt palgatud isikuga. Sel juhul tuleb aga tagada teadmuse jäämine KOVi ja nõuda tegevuse pidevat dokumenteerimist.
- **Personalispetsialist** – koordineerib personaliturbe teemasid.

- **Haldusspetsilist** – koordineerib füüsilise turbe teemasid.
- **IT-spetsialist** – koordineerib infotehnilist turvet, konsulteerib andmekogude omanikke, abistab IT-ga toimetulemist, koostab/kooskõlastab ITga seotud dokumentatsiooni ja hoiab seda ajakohasena.
- **Juhtkonna esindaja** – korraldab ressursse ja kinnitab tehtud töid, motiveerib teisi, ideaalis kattub see roll ISKE rakendamise koordinaatoriga.
- Struktuuriüksuste juhid või muud **võtmeisikud** – enamasti andmekogude omanikud, kelle kaudu ISKE meetmete rakendamine toimuda saab.
- **Sisekontroll** – koordineerib ISKE rakendamise järelevalvet ja teostab ISKE meetmete rakendatuse analüüsi oma pädevuste piires.
- **Infoturbe spetsialist** – vastutav turvalahenduste plaanimise, kasutusele võtu ja toimimise eest, sageli IT-spetsialistiga sama isik.
- **Isikuandmete kaitse eest vastutav isik** – vastavalt IKS nõuetele, peab olema sõltumatu järelevalvatavate andmete töötlusest.
- **RIHA administraator** – kannab KOVi andmekogudega seonduva info RIHAsse.

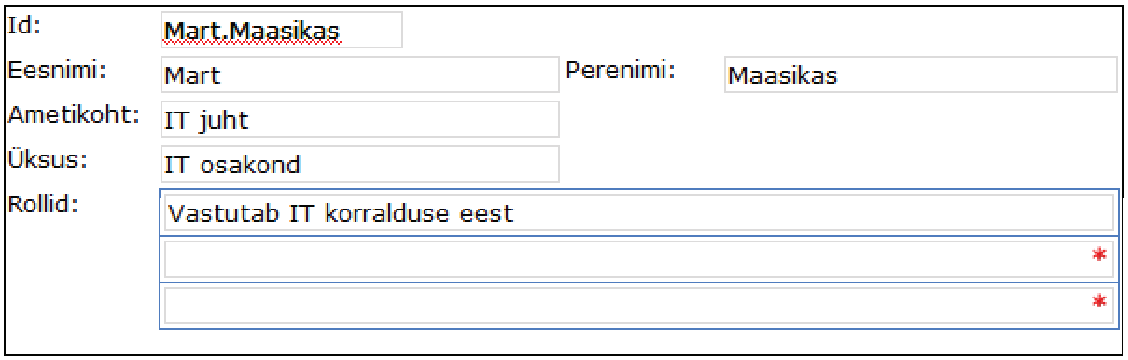
ISKE rakendamise töörühm ei tohi kohapeal koosneda vaid ühest inimesest. Sisekontrolli roll ISKE rakendumise käigus üha enam tähtsustub. Võimalik, et edaspidi leitakse võimalusi sisekontrolli rolli tekitamiseks kas mitmete KOV-de peale ühiselt või suuremates KOV-des kohtadel, kes kannaks samaaegselt ka isikuandmete kaitse eest vastutava isiku rolli.

### 5.1.2 Inventuuri etapp 1: Kasutajad

Infovarade inventuuri läbiviimise korraldab ISKE koordinaator, osalema peaks IT-spetsialist ja andmekogude fikseerimisel on oluline kaasata kõik asutuse võtmeisikud.

Enne infovarade spetsifitseerimist tuleks viitamise lihtsustamiseks üles loetleda kõik infovarade kasutajad. Kasutajate kohta tuleks koguda järgmised andmed:

- Eesnimi
- Perenimi
- Ametikoht
- Üksus
- Kasutaja rollid (nt ISKE koordinaator)



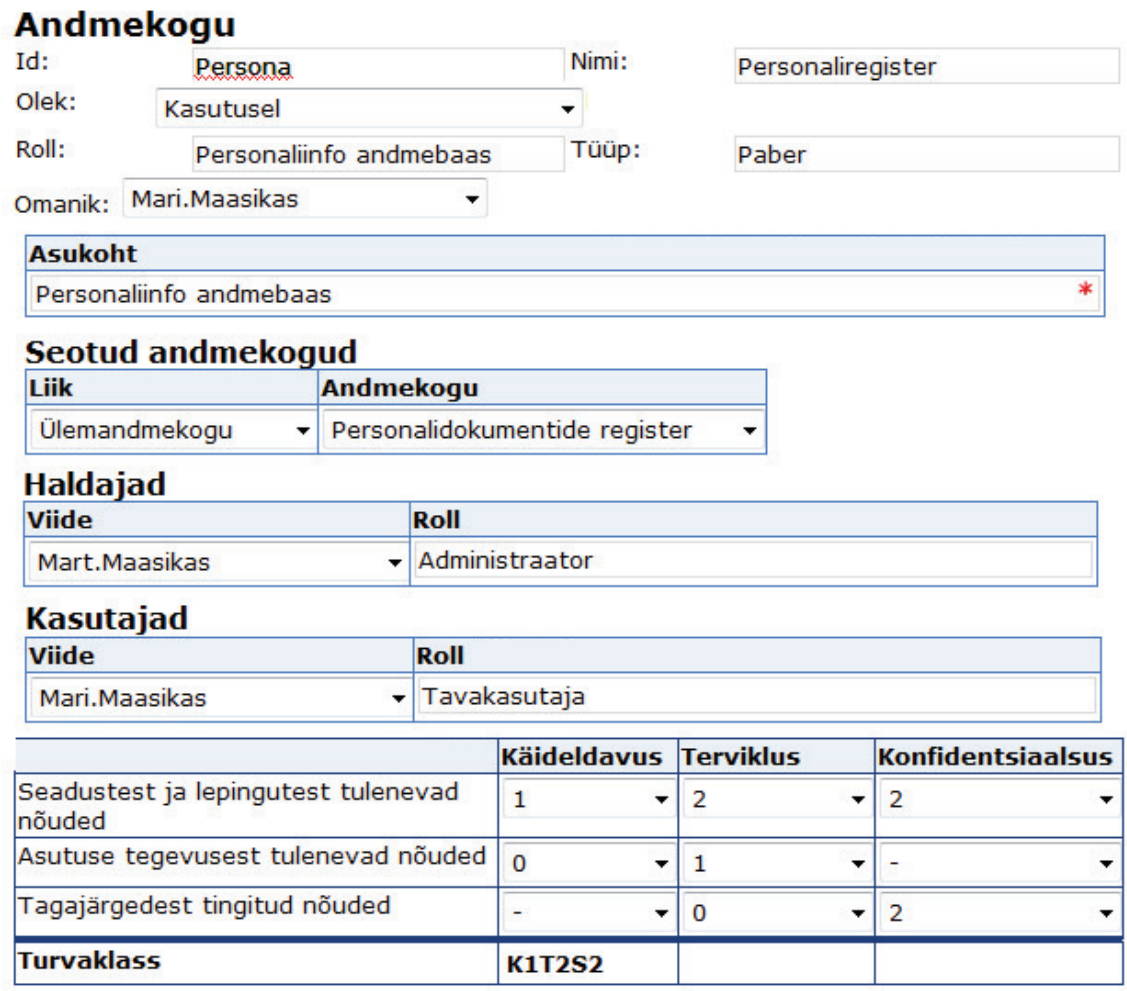

**Joonis 4. Näidisvorm kasutaja andmete kogumiseks**

Kasutajaid on mugav grupeerida kasutajagruppidesse (nt struktuuriüksuste järgi Sotsiaalosakond, personaliosakond, raamatupidamine jne), millele saab hiljem infovarade juures viidata. Vajadusel/võimalusel võiks lisada kasutaja kontaktandmed.

### 5.1.3 Inventuuri etapp 2: Andmekogud

Seejärel tuleks üles loetleda andmekogud. Andmekogude kohta tuleb koguda järgmisi andmeid:

- Andmekogu nimetus (Nimi)
- Roll (kasutamise eesmärk)
- Olek (arhiveeritud, kasutusel, testimisel või plaanitud)
- Andmekogu tüüp (paber, failid, andmekogud, varukoopia, muu)
- Omanik (viidata eelnevalt üles loetletud kasutajale)
- Asukoht (andmebaas, server, kapp, ruum, asutus), kus andmekogu asub (võib täita hilisemas etapis viitega).
- Andmekogu administraatorid (viidata eelnevalt üles loetletud kasutajatele) ja rollid
- Andmekogu kasutajad (viidata eelnevalt üles loetletud kasutajatele, kasutajagruppidele) ja rollid
- Andmekoguga seotud andmekogud (alamandmekogud ja ülemandmekogud)
- Andmekogule esitatud turvalisuse nõuded seadustest ja lepingutest, asutuse tegevusest, nõuded tagajärgedest väljendatuna turvaosaklassidena (turvavajadus turvaklassidena lisatakse hiljem).




**Joonis 5. Näidisvorm andmekogu kohta andmete kogumiseks**

Lisaks võiks ISKE järjepideva rakendamise ja rahvusarhiivi nõuete rahuldamise eesmärgil märkida ära ka

- andmekogu asutamise aeg,
- andmekogu kasutuselt eemaldamise aeg,
- andmete ajaline piir (millisest ajast andmeid andmekogusse kogutakse),
- säilitustähtaeg,
- sisu täpsustus,
- tüüp (andmete lisamine jooksvalt, andmete ülekirjutamine).

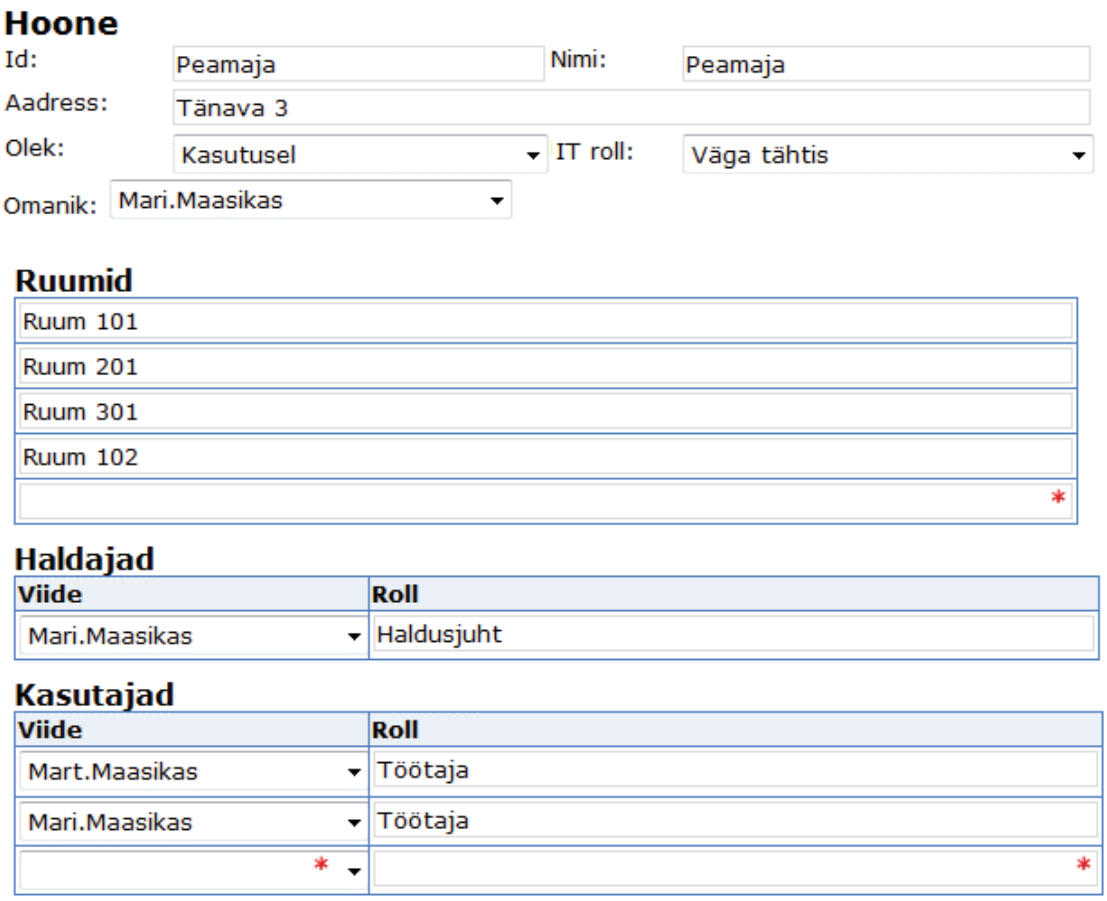
Andmekogude üks näidisloend on esitatud:
http://dw.riik.ee/KOV_IS_turvameetmete_tohustamine/KOV_andmekogud .

Andmekogude loendi alusena võib käsitleda ka aruande elektroonilise lisana esitatud ja Viljandi LV-s kasutusel olevat andmekogude spetsifikatsiooni alustabelit.

### 5.1.4 Inventuuri etapp 3: Hooned

Järgnevalt tuleb kokku lugeda infrastruktuuri varad. Alustada on soovitav hoonete üles lugemisest. Hoonete kohta tuleb koguda järgmist infot:

- Identifikaator (nt peamaja)
- Nimi
- Aadress
- Olek (kasutusel, testimisel või planeeritud)
- IT roll (toetav, asjakohane, väga tähtis, eluliselt tähtis, tähtsusetu)
- Omanik (viide kasutajale – rollitäitja, kes vastutab maja füüsilise turbe eest)
- Hoones olevad ruumid (täita järgmises etapis viidetega ruumidele)
- Hoone haldajad (viited kasutajatele, kes viivad läbi haldustegevusi nt tuleohutus, võtmetehaldus, valve, koristusteenus jne)
- Hoone kasutajad (viited kasutajatele või kasutajagrupile)




**Joonis 6. Näidisvorm hoonete kohta andmete kogumiseks**

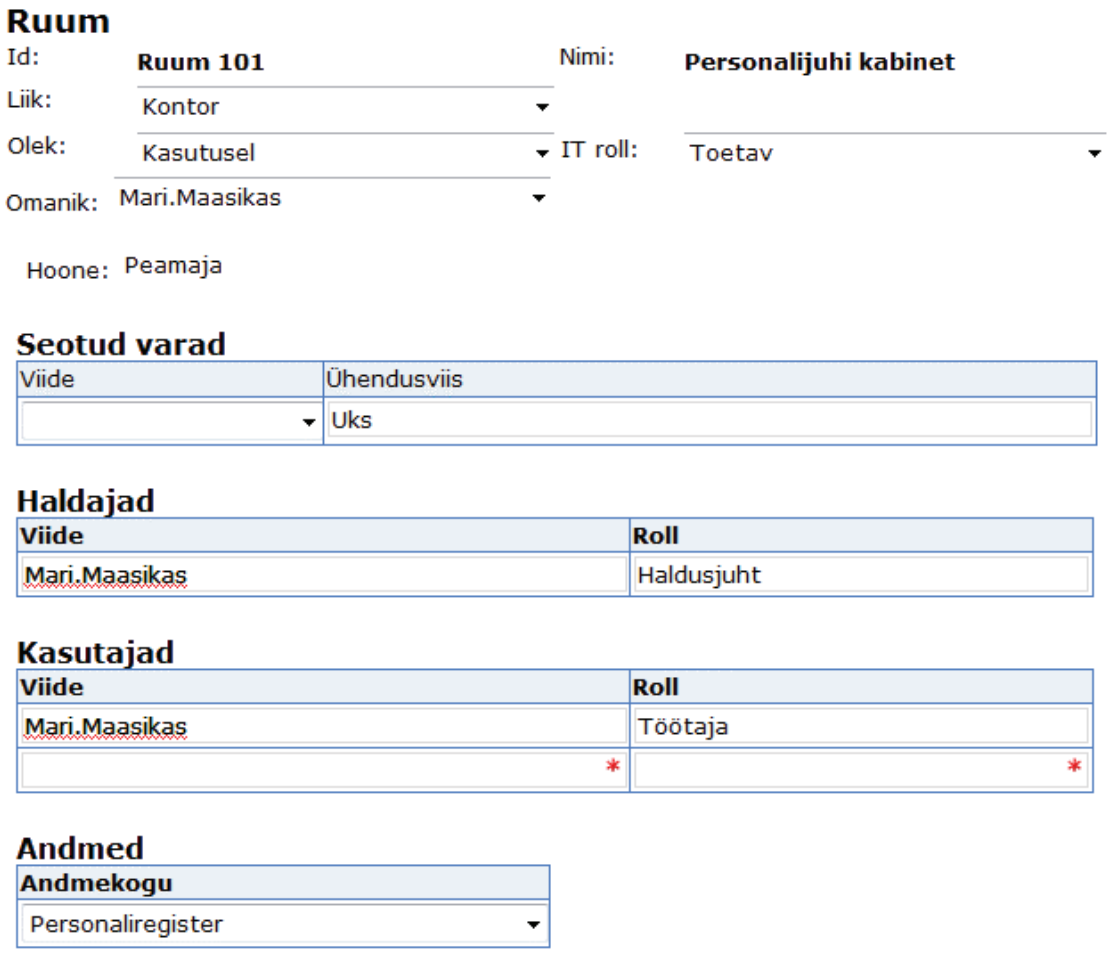
Ka hoonete puhul tuleks ISKE järjepidevuse saavutamiseks märkida juurde hoonete kasutuselevõtu ja kasutuselt eemaldamise ajad.

### 5.1.5 Inventuuri etapp 4: Ruumid

Hoonetes asuvate ruumide kohta tuleb koguda järgmist infot:

- Ruumi identifikaator

- Nimi
- Asukoht (viide hoonele)
- Olek (kasutusel, testimisel või planeeritud)
- Liik (serveriruum, koosolekuruum, koolituste ruum, ürituste ruum, tehnilise infrastruktuuri ruum, kontor, koridor, muu)
- IT roll (toetav, asjakohane, väga tähtis, eluliselt tähtis, tähtsusetu)
- Omanik (viide kasutajale)
- Ruumi haldajad (viited kasutajatele)
- Ruumi kasutajad (viited kasutajatele või kasutajagrupile)
- Ruumis olevad infovarad (võib täita hilisemas etapis viidetega)
- Muud seosed teiste infovaradega (nt. ühendatud uksega teise ruumiga):
    - Viide seotud varale
    - Seose tüüp (nt lukustamata uks, lukustatav ametikäik, lukustatav uks, tuletõke)
- Ruumis olevate andmekogude loetelu (viited)




**Joonis 7. Näidisvorm ruumide kohta andmete kogumiseks**

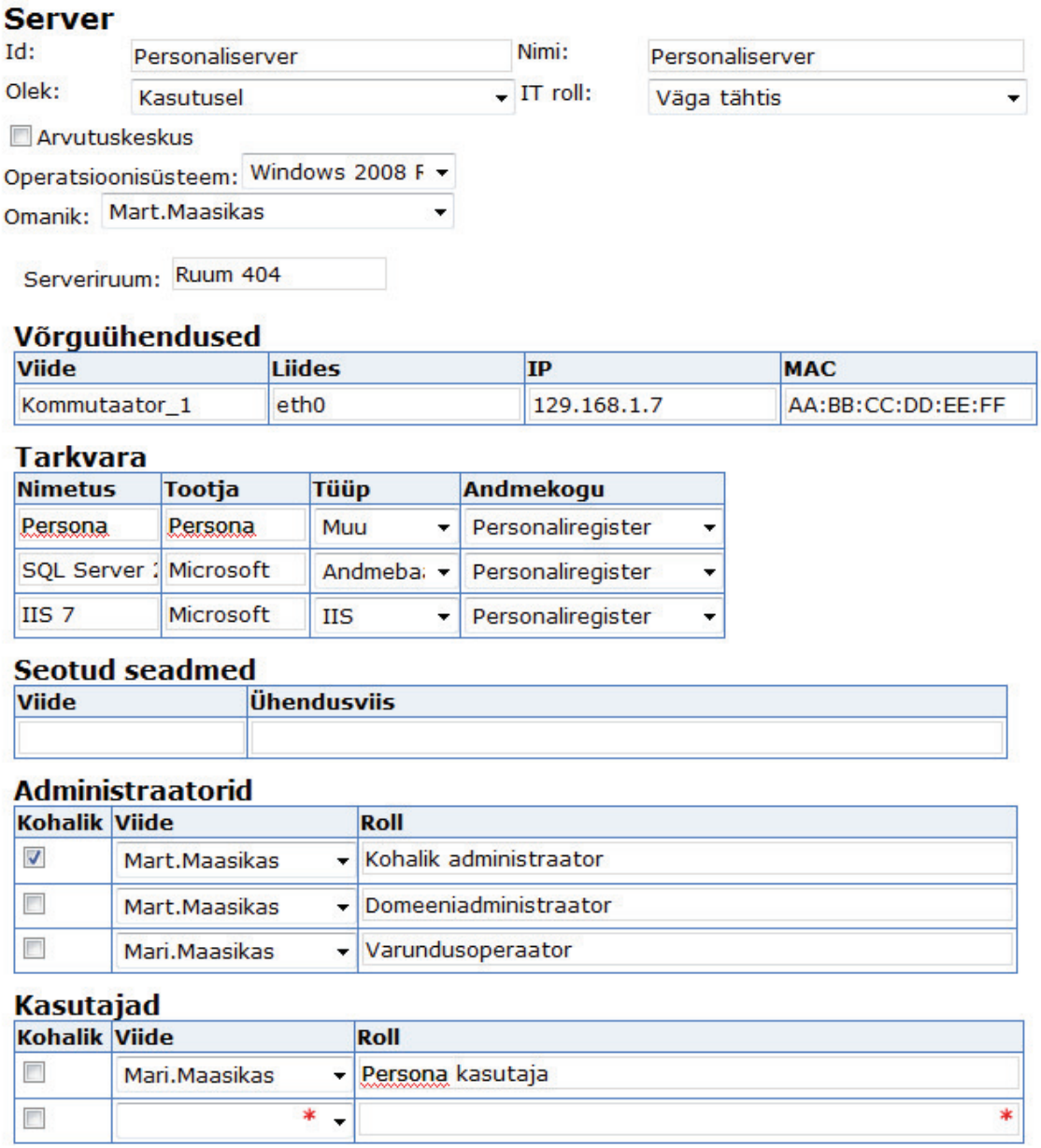
Ka ruumide puhul tuleks ISKE järjepidevuse saavutamiseks märkida juurde kasutuselevõtu ja kasutuselt eemaldamise ajad.

### 5.1.6 Inventuuri etapp 5: Serverid

Serverid on kõik arvutivõrgus teenuseid pakkuvad füüsilised ja virtuaalsed seadmed (ka ISDN keskjaam, võrguprinter, klaster ja andmebaasi serveeriv personaalarvuti on serverid). Projektiga kaasnevatest seadmetest on serveritena käsitletavad Synology DS209+II (NAS) ja Juniper SSG-5 (lüüs). Serverite kohta tuleb koguda järgmist infot:

- Identifikaator
- Nimi
- Olek (kasutusel, testimisel või planeeritud)
- IT roll (toetav, asjakohane, väga tähtis, eluliselt tähtis, tähtsusetu andmekogu käitlemise seisukohast)
- Omanik (viide kasutajale)
- Administraatorid (viited kasutajatele) rollide (nt varunduse administraator, operatiivne administraator, muu) ja kontoliikidega (kohalik, keskne)
- Kasutajad (viited kasutajatele või kasutajagrupile) rollide ja kontoliikidega
- Operatsioonisüsteem (Windows 2008 R2/7, Windows 2008/Vista, Windows 2003/XP, Windows 2000, Windows NT, Vanem Windows, IBM suurarvuti, Unix/BSD/Linux, Novell Netware, Muu)
- Kas tegemist on arvutuskeskusega
- Kas server kuulub klastrisse või grid-i ning viide sellele (grid või klaster on eraldi serverina loetletav)
- Asukoht (viide serveriruumile, kaitsekapile või ruumile)
- Võrguühenduste loetelu:
    - Viide ühendatud seadmele (võib lisada hilisemas etapis, loetleda vaid otseseid füüsilisi või loogilisi seoseid)
    - Liides (nt eth0)
    - IP-aadress
    - MAC-aadress
- Muude ühenduste loetelu (nt ühendatud printer, UPS, Modem, külalisserver (*guest*), peremeesserver (*host*))
    - Viide ühendatud seadmele (võib lisada hilisemas etapis)
    - Ühendusviis/seos (nt USB, külalisserver (*guest*), peremeesserver (*host*))
- Loetelu serveri (operatsioonisüsteemi) poolt käideldavate andmekogudega (Viited)
- Serveris kasutatava tarkvara loetelu:
    - Tarkvara nimetus

- Tarkvara tootja
- Tarkvara käideldavate andmete liik (paberi, failid, andmekogu, varukoopia, muu)
- Tarkvara tüüp (Turvalüüs/Tulemüür, Marsruuter, Kommutaator, Salvestisüsteem, Varundusserver, Failiserver, ISDN kesksidesüsteem, Faksiserver, Printserver/Skänner, Automaatvastaja, Lotus Notes Server, Exchange Server, Muu E-posti server, IIS, Apache, Muu veebiserver, Andmebaasiserver, Kaugligipääs, Novell eDirectory, Active Directory, Muu kataloogiteenus (nt OpenLDAP), SAP, VPN server/lüüs, Telefon (GSM), IP-Telefon, Outlook, Lotus Notes klient, Muu e-posti klient, kontoritarkvara, Workgroups for Windows tipp, Muu)
- Vajadusel viide andmekogule




**Joonis 8. Näidisvorm serverite kohta andmete kogumiseks**

Ka serverite puhul tuleks ISKE järjepidevuse saavutamiseks märkida juurde kasutuselevõtu ja kasutuselt eemaldamise ajad.

### 5.1.7 Inventuuri etapp 6: Klientarvutid

Klientarvutid on tavaliselt personaalarvutid, kuid ka mobiiltelefonid, sülearvutid, „netbook“ arvutid, pihuarvutid ja teised „targad“ võrguseadmed. Klientarvutite puhul eristatakse eraldi „Internet PC“-d, mis on arvuti, millel puudub ligipääs sisevõrku, kuid on olemas ligipääs välisvõrku (nn “internetipunktid”). Klientarvutite kohta tuleb koguda järgmist infot:

- Identifikaator
- Nimi
- Olek (kasutusel, testimisel või planeeritud)
- IT roll (toetav, asjakohane, väga tähtis, eluliselt tähtis, tähtsusetu)
- Omanik (viide kasutajale)
- Administraatorid (viited kasutajatele) rollide (nt varunduse administraator, operatiivne administraator, muu) ja kontoliikidega (kohalik, keskne)
- Kasutajad (viited kasutajatele või kasutajagrupile) rollide ja kontoliikidega
- Operatsioonisüsteem (Windows 2008 R2/7, Windows 2008/Vista, Windows 2003/XP, Windows 2000, Windows NT, Vanem Windows, Unix/BSD/Linux, Muu)
- Kas arvuti on mobiilne
- Kas tegemist on Interneti PC-ga
- Asukoht (viide ruumile või kasutajale, kellele see kasutada on antud)
- Võrguühenduste loetelu:
    - Viide ühendatud seadmele (võib lisada hilisemas etapis, loetleda vaid otseseid füüsilisi või loogilisi seoseid)
    - Liides (nt. eth0)
    - IP-aadress
    - MAC-aadress
- Muude ühenduste loetelu (nt ühendatud printer, UPS, Modem, külalisserver (*guest*), peremeesserver (*host*))
    - Viide ühendatud seadmele (võib lisada hilisemas etapis)
    - Ühendusviis/seos (nt. USB, külalisserver (*guest*), peremeesserver (*host*))
- Loetelu arvuti (operatsioonisüsteemi) poolt käideldavate andmekogudega (viited andmekogudele)
- Arvutis kasutatava tarkvara loetelu:
    - Tarkvara nimetus
    - Tarkvara tootja

- Tarkvara poolt käideldav andmekogu (viide)
- Tarkvara tüüp (Turvalüüs/Tulemüür, Marsruuter, Kommutaator, Salvestisüsteem, Varundusserver, Failiserver, ISDN kesksidesüsteem, Faksiserver, Printserver/Skänner, Automaatvastaja, Lotus Notes Server, Exchange Server, Muu E-posti server, IIS, Apache, Muu veebiserver, Andmebaasiserver, Kaugligipääs, Novell eDirectory, Active Directory, Muu kataloogiteenus (nt. OpenLDAP), SAP, VPN server/lüüs, Telefon (GSM), IP-Telefon, Outlook, Lotus Notes klient, Muu e-posti klient, kontoritarkvara, Workgroups for Windows tipp, Muu)

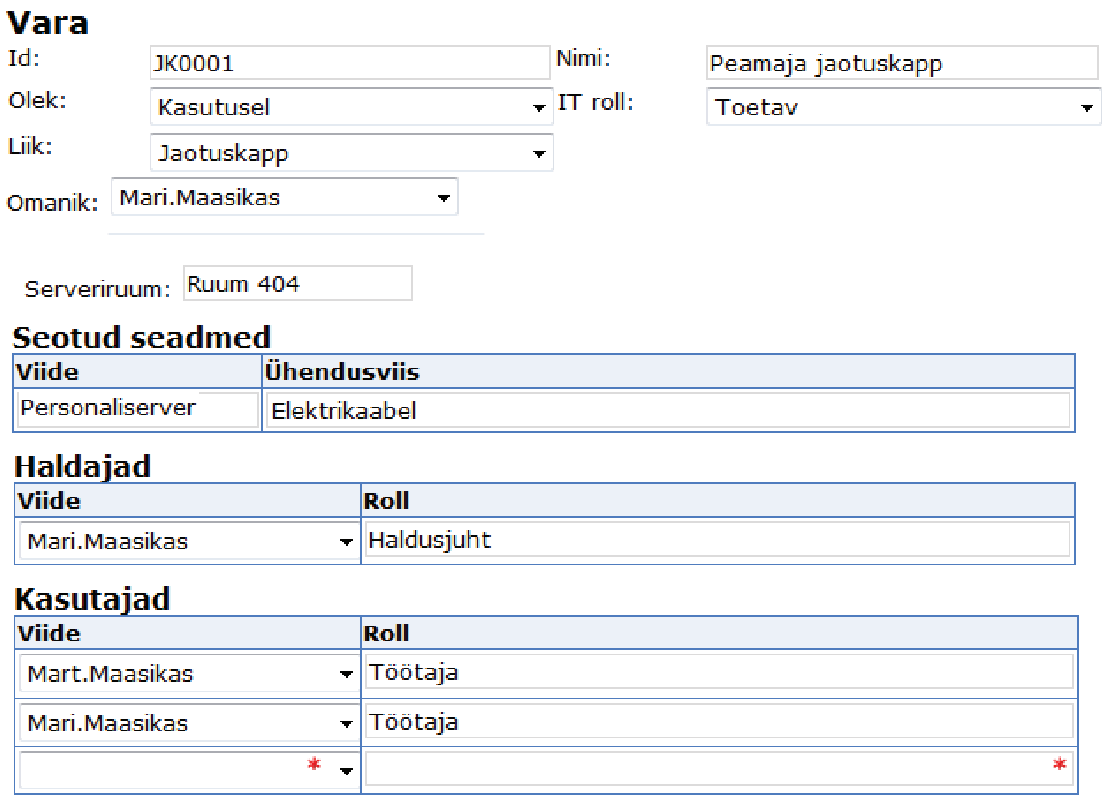

**Joonis 9. Näidisvorm klientarvuti kohta andmete kogumiseks**

Ka klientarvutite puhul tuleks ISKE järjepidevuse saavutamiseks märkida juurde kasutuselevõtu ja kasutuselt eemaldamise ajad.

### 5.1.8 Inventuuri etapp 7: Muud varad

Muude varade hulka käivad printerid, kaitsekapid, võrguseadmed, andmekandjad, kaabeldused (IT ja elektrotehnilised eraldi) ja muud varad, mis eelpool olevatesse kategooriatesse ei kuulu. Projektiga kaasnevatest seadmetest on muude varadena käsitletavad Cisco ESW520-24 (hallatav võrgulüliti) ja seadmekapid. Nende varade kohta tuleb koguda järgmist infot (olenevalt vara tüübist):

- Identifikaator
- Nimi
- Olek (kasutusel, testimisel või planeeritud)
- IT roll (toetav, asjakohane, väga tähtis, eluliselt tähtis, tähtsusetu)
- Liik (kaitsekapp, kaitsmekapp, printer, modem, faks, telefon, mobiilne andmekandja, statsionaarne andmekandja, IT kaabeldus, elektrikaabeldus, marsruuter, võrgulüliti, muu)
- Omanik (viide kasutajale)
- Administraatorid (viited kasutajatele) rollidega (nt varunduse administraator, operatiivne administraator, muu)
- Kasutajad (viited kasutajatele või kasutajagrupile) rollidega
- Asukoht (viide ruumile või kasutajale, kellele see kasutada on antud)
- Võrguühenduste loetelu (kui omab võrguühendusi):
    - Viide ühendatud seadmele (võib lisada hilisemas etapis, loetleda vaid otseseid füüsilisi või loogilisi seoseid)
    - Liides (nt eth0)
    - IP-aadress
    - MAC-aadress
- Muude ühenduste loetelu (nt ühendatud arvutiga)
    - Viide ühendatud seadmele
    - Ühendusviis/seos (nt USB)
    - Loetelu vara poolt käideldavate andmekogudega (kui käitleb andmeid, viited andmekogudele)




**Joonis 10. Näidisvorm muude varade kohta andmete kogumiseks**

Ka muude varade puhul tuleks ISKE järjepidevuse saavutamiseks märkida juurde kasutuselevõtu ja kasutuselt eemaldamise ajad.

Inventuuri etapi järgselt on kasulik kontrollida inventuuri korrektsust võrguskeemi abil, et veenduda kõigis olemasolevates seostes ja andmete liikumise teedes infotehnoloogiliste vahendite abil. Ka elektrotehniliste võrkude skeemide omamine kohtadel on oluline, et tagada ka aastate pärast oluline teadmus juhtemestuse kohta, kui võimalik hetkel pädev isik on asutusest lahkunud.

### 5.1.9 Turvaosaklasside määramine

Pärast inventuuri teostamist tuleb määrata infovarade turvavajadus ehk ISKE metoodika järgi **turvaosaklassid**. Turvaosaklasside põhjal saadakse kokku **turvaklass** (nt K1T1S2). Andmete **omanikud** määravad andmekogudele turvaklassid kolme turvaosaeesmärgi (käideldavus **K**, terviklus **T** ja konfidentsiaalsus **S**) järgi, lähtudes

- seadustest ja lepingutest tulenevatest nõuetest,
- põhitegevusest tulenevatest vajadustest ja
- tagajärgede kaalukusest.

**NB!** Turvaklassi määrab andmekogule andmete omanik konsulteerides IT-spetsialistiga (vt elektrooniline lisa andmekogudele turvaklasside määramise ankeet).

Füüsilistele infovaradele määratavate turvaklasside aluseks on andmekogule määratud turvaklassid ning ISKE rakendusjuhendi punkt 2.3. Edasises analüüsis tuleks sama tüüpi samade nõuetega varad grupeerida (nt tekiksid grupid nagu peamaja printerid, sülearvutid,

lauaarvutid, koosolekuruumi arvutid, kommutaatorid, marsruuterid, jne). Grupeerimisel võib lisada ka eraldi jaotuse:

- Andmekogusid käitavad infovarad (sisuliselt serverid, mis on eluliselt tähtsad andmete igasuguseks töötlemiseks),
- Andmekogusid käitavaid infovarasid toetavad infovarad (võimaldavad/toetavad pääsu andmeteni),
- Autonoomsed infovarad – pole otseselt võrku ühendatud, kuid on olulised andmetöötluse seisukohast.

Muude infovarade turvaklass tuletatakse toetusastme järgi (infovarade spetsifikatsioonis mõiste *IT roll*), võttes aluseks kõrgeimad infovaradega seotud andmekogudele määratud turvaosaklassid. Kui toetusaste on eluliselt tähtis või tähtis, jääb turvaklass samaks andmekogu turvaklassiga, kui vaid toetav, siis võib turvaklass olla astme võrra madalam. Nt kui määrata turvaklassi IT kaabeldusele, siis tuleb arvestada kõige kõrgemate andmekogude turvaklassidega, mis vastavat kaabeldust andmete edastuseks kasutavad ja hinnata toetusastet. Tavaliselt on see kaabelduse puhul eluliselt tähtis. Seega oleks IT kaabelduse turvaklass samane kõrgeimate andmekogudele määratud osaklassidega. Samas nt printer ei pruugi olla andmekogu jaoks eluliselt tähtis, sel juhul kui andmekogudele oli määratud turvaklassiks K2T2S2, siis printeri turvaklassiks võime määrata K1T1S1.

Varad, mis otseselt pole andmekogudega seotud, kuid võivad mängida siiski olulist rolli andmetöötluses (sh protsessid ja muud organisatsioonilised teemad ISKEs kajastatud B1 moodulis), siis neile määratakse mitte turvaklass, vaid turbeaste vastavalt kõrgeima andmekogudele määratud turvaosaklasside järgi. Kui kõrgeimatest turvaosaklassideks olid nt erinevatel andmekogudel K1T1S2 ja K2T1S1, siis vastavalt ISKE jaotises 3.1 turvaklasside ja turbeastmete vaheliste seoste tabelile, oleks sel juhul turbeastmeks M (keskmine).

## 5.2 SAMMUD 6–7: RAKENDATAVATE MEETMETE MÄÄRAMINE

Tööde teostamisel osalevad ISKE koordinaator koostöös IT-spetsialisti ja haldusjuhiga. Infovarade ja nendele vastavate moodulite tuvastamisel saab kasutada aruande lisades B–D toodud maatrikseid. Nendes maatriksites on eelnevatel sammudel spetsifitseeritud infovarade tüüpidele (veerud) pandud vastavusse tüüpmoodulid (read). Kollane kolmnurk tähistab, et tüüpmoodul rakendub vaid osadel juhtudel. Seda, kas tüüpmoodulit tuleb rakendada või mitte, saab tuvastada tüüpmooduli kirjelduse põhjal ISKE kataloogis. Tüüpmoodulite tähised tuleb kirjeldada vastava infovara/infovaragrupi juurde (nt tähis B2.301).

Maatriksi „Infrastruktuur ja võrk“ juurde käivad järgmised kommentaarid:

- Bürooruumi puhul tuleb rakendada tüüpmoodulit B 2.4 „Serveriruum“, kui ruumis leidub servereid. NB! Serveriks loetakse ka otse võrku ühendatud võrguteenuseid pakkuvaid seadmeid (nt multifunktsionaalne seade (kontorikombain)).
- Kui andmekandjate arhiiv sisaldab pabereid või filme, tuleb rakendada ka vastavaid soovituslikena märgitud meetmeid andmekandjate arhiivi kohta.

- Tehnilise infrastruktuuri ruum on ruum, kus on seadmed, mis vajavad inimeste poolset hooldamist harva. Juhul kui selles ruumis on servereid, tuleb sellele ruumile rakendada ka serveriruumi tüüpmoodulit.
- Kaitsekappi saab kasutada serveriruumi või andmekandjate arhiivi asemel.
- Mobiilne töökoht on väljaspool kontorit või kodukontorit asuv töökoht, nt sülearvuti kasutamine kliendi juures.
- Üldkasutatavad ruumid on koolituste, koosolekute ja ürituste ruumid, kuhu pääsevad aeg-ajalt ka võõrad (st mitte asutuse töötajad).

Maatriksi „IT süsteemid“ juurde käivad järgmised kommentaarid:

- Tüüpmoodul B 3.202 „Autonoomne IT-süsteem“ rakendatakse seadmetele, mis pole ühendatud arvutivõrku.
- Interneti PC on arvuti, millel puudub pääs sisevõrku, kuid on olemas pääs välisvõrku, nt kiosk tüüpi süsteemid.
- ISKE mõistes on ka CIFS/SAMBA (Windowsi failide jagamine/failiserver) NAS (võrgusalvestisüsteem).

Maatriksi „Rakendused“ juurde käivad järgmised kommentaarid:

- Mooduli B 5.1 „Võrdõigusteenus“ all mõeldakse Windowsi failide jagamist ilma serverita (Windows for Workgroups).
- Mobiilsed andmekandjad (CD, DVD, mälupulgad) alla kuuluvad ka mp3 mängijad, mobiiltelefonid, diktofonid, fotoaparaadid ja videokaamerad.
- Faksiserverite alla kuuluvad ka e-postiga integreeritud faksi teenust pakkuvad tooted.

Lisades olevad maatriksid on abimaterjalid infovarade sidumisel tüüpmoodulitega. Maatriksi kasutamine ei taga kõigi teemakohaste moodulite määramist, moodulite määramisel tuleb määrajal ise käia kriitilise suhtumisega üle tüüpmoodulite loend, et sealt tuvastada mooduleid, mis võivad täiendavalt olla asjakohased. Tüüpmoodulite tuvastamise järel saab infovaradega siduda vastavalt turbeastmele asjakohased turvameetmed.

Kasutades ISKE rakendustööriista, selekteeritakse vastavad meetmed kasutaja eest automaatselt (eelduseks korrektne infovarade inventuur, infovarade seosed andmekogudega, infovarade turvaklassid ja infovarade sidumine tüüpmoodulitega). Vastasel juhul tuleb see teostada käsitsi ISKE kataloogide abil.

Erandiks on ISKE tüüpmoodul B1, mille meetmed rakendada sõltumatult infovaradest kõrgeimal tuvastatud andmekogu turvaastmel.

## 5.3 SAMMUD 8–9: RAKENDAMISE PLAANIMINE JA TÄITMINE

ISKE rakendamine nõuab mitmete dokumentide loomist. Dokumentatsiooni koostamise eelduseks on olemasolevatest sisemistest regulatsioonidest ja juhistest eelnev ülevaate saamine. Käesoleva dokumendi lisades on toodud näidismallid mõnede levinud dokumentide jaoks. Üldine infoturbepoliitika mall (aruande lisa) annab juhtnööre turvapoliitika koostamiseks kohtadel. Turvapoliitika peab olema elus dokument, seega

oleks lubamatu dokumendi kehtestamine ilma omapoolsete oluliste muudatusteta. Sama kehtib ka kõigi teiste näidisdokumentide kohta.

Kõigi näidisdokumentide realiseerimine kohtadel ei pruugi olla otstarbekas. Vajalik on leida kohal puuduv ja muu dokumendiga mitteasendatav, kuid siiski oluline infokogum.

**Üldine kommentaar dokumentatsiooni kohta:**

Loodaval ja käigusoleval dokumentatsioonil peab olema konkreetne vastutaja/omanik, kelle ülesanne on vastava dokumendi ajakohastamine ja iga-aastase läbivaatuse korraldamine. Dokumente pole mõtet kasutusse võtta, kui nende eest keegi ei vastuta. Oht on, et dokumentatsioon vananeb väga kiiresti ja on sisuliselt kasutu, sellesse algselt investeeritud ressurss oli tegelikult vaid formaalsuse täitmiseks. Pigem omada vähem, aga ajakohast ja tegelikkusega vastavuses olevat dokumentatsiooni, kui luua dokumente vaid nende loomise eesmärgil.

Seega:

- Igal dokumendil on omanik.
- Iga dokumenti vaatab omanik läbi ja vajadusel ajakohastab kord aastas või suuremate muutuste või intsidentide korral.
- Dokumendi loomisel pole mõtet, kui see luuakse vaid formaalsuse täitmiseks.

**Rakendusplaan**

ISKE meetmetest rakendusplaani koostamiseks on esmatähtis saada ülevaade meetmetest, mis on juba rakendatud või rakendamisel.

Meetmed, mis pole rakendatud täielikult, tuleb kajastada rakendusplaanis (ISKE tööriista puhul on see üks raporti vorm). Rakendusplaanis tuleb fikseerida:

- Rakendatava meetme(te) tähis(ed) (mõnikord terve mooduli tähis)
- Rakendamise eest vastutaja
- Rakendamiseks vajalik ressurss (aeg ja raha)
- Rakendamise tähtaeg (kas regulaarsed tähtajad nt tulekustutite taatlemine)
- Detailne rakendamise informatsioon (kommentaari detailsus sõltub meetme spetsiifikast).

Rakendusplaanis nimetatakse sageli ka rakendamise prioriteet.

Rakendamise plaan peab saama juhtkonna heakskiidu!

Rakendamise plaani koostamine on kogu ISKE töörühma koostöö tulem, töö tulemi eest vastutab aga siiski ISKE koordinaator.

Hetkel on RIA poolt väljatöötatud ISKE auditeerimise juhend. Auditeerimise juhendis on pakutud välja rakendatuse määra klassifikaatorid (vt http://ria.ee/27220).

Vastavad klassifikaatorid saavad olema ka ISKE rakendustööriistas.

**NB!** ISKE meetmete rakendamisel tuleb lähtuda mõistlikkuse ja piisavuse printsiibist. Kõigi meetmete 100% rakendamine pole enamasti võimalik ja otstarbekas. Meetmete kataloogi mõte on, et olulised teemad ei ununeks ja saaksid kinnituse, et kõik lahendused on läbi mõeldud. Meetmeid, mida ei rakendata, tuleb põhjendada – miks ei rakendata (nt riski vähendatakse muude alternatiivmeetmetega). Kui KOVi juhtkond aktsepteerib kaasnevat riski ja omab piisavat reservfondi riski realiseerumisel, siis on oluline see fikseerida, et oleks teada, miks, millal ja kelle poolt nii otsustati. Vastav otsus tuleb vähemalt kord aastas üle vaadata. Samuti tuleb põhjalikult analüüsida kõiki turvaintsidente, et veenduda organisatsiooni infoturbe piisavuses.

## 5.4 SAMM 10: JÄRJEPIDEVA ISKE RAKENDATUSE TAGAMINE

ISKE rakendamine on tsükliline protsess, st et ISKE rakendamine on käsitletav projektina vaid esmakordsel ISKE rakendamisel, edaspidi on tegu ISKE käigushoidmisega.

ISKE käigushoidmine tagatakse, kui

- koostatakse regulaarseid infoturbe ülevaateid juhtkonnale,
- uuendatakse infovarade nimekirja vastavalt infovarade muutumisele,
- peetakse intsidentide registrit,
- järgitakse ISKE rakendatuse plaani ja seda ajakohastatakse,
- fikseeritakse õigusaktidega kaasnevaid turvanõudeid ja arvestatakse nendega KOVi töö korraldamisel,
- vähemalt kord aastas teostatakse dokumentatsiooni läbivaatust ja uuendamist,
- vähemalt kord aastas vaadatakse läbi kõik turvameetmed kooskõlas ohtude kataloogiga, (eesmärk on veenduda, et uusi ohte pole lisandunud ja rakendatud meetmed täidavad oma eesmärki),
- kõiki tulemeid tutvustatakse vajalikele huvigruppidele - teadlikkustamine,
- kehtestatud infoturbe nõuete täitmist kontrollitakse pidevalt ja meetmete täitmist motiveeritakse nii koolituste kui motiveeriva käitumisega (eriti juhtkonna esindajate poolt) - turvalise käitumiskultuuri tekitamine ja säilitamine.

ISKE meetmete läbivaatust on soovitav teostada enne järgmise aasta eelarve koostamist, et vajadusel läbivaatuse tulemeid saaks eelarve koostamisel arvestada. Seega saab läbivaatus kindlad ajalised raamid.