Turvaanalüüsi metoodikate hindamine ja astmelise etalonturbe juhendmaterjal

Jüri Kivimaa

21. juuni 2004

SISUKORD

1. TÖÖÜLESANNE

1. Töö sisuks on soovituste andmine süsteemseks lähenemiseks infoturbe metoodikate koostamise ja kohaldamise valdkonnas ettevõtte või infosüsteemi tasemel. Töö peab lähtuma eelkõige praktilistest infoturbe korralduse vajadustest. Tuleb osutada ka turvaauditi metoodikate eripärale ning valdkonna õigusliku reguleerimise võimalustele. Töös tuleb anda soovitusi analüüsi läbiviimiseks infoturbe eesmärkide ja vajaduste väljaselgitamisel ning turvanõuete püstitamisel.

Tuleb hinnata meetodeid ja strateegiaid, mis võiks asutustes infosüsteemide turvaanalüüsi tegemisel abiks olla, pidades silmas alljärgnevat:

- täpsustada ja piiritleda turvaanalüüsi mõiste, defineerida mõiste sisu ja tähendus
- esitada täiendavad soovitused andmeturbe eesmärkide ja nende tasemete määratlemiseks

2. Töö teise osa moodustab astmeliste etalonturbe meetmete metoodilise juhendmaterjali täiendamine ja ajakohastamine, kasutades astmelise metoodika juurutamise ja standardite kohaldamise praktilisi tulemusi Eesti avaliku sektori ametiasutustes. Infosüsteemidele määratud turvaklasside adekvaatsusest sõltub õigete turvameetmete valik etalonmeetmete kataloogist. Seega tuleb käesolevas töös pöörata erilist tähelepanu analüüsiprotseduuri rollide ja tegevustega seonduvale.

Töös antakse astmelise etalonturbe otstarbeka kohaldamise juhised ettevõtete probleemide lahendamisel. Etalonturbe käsitluse laiendamine, turvameetmete otstarbekas häälestamine detailanalüüsi tulemusena leitud olulistel lõikudel. Töö tulemusena saame abivahendi ka andmekogu või registri andmete spetsifikatsiooni koostamisel ning etalonturvameetmete rakendamisel. Lähtuda tuleb majandusliku otstarbekuse loogikast.

2. TURVAANALÜÜSI METOODIKATE HINDAMINE

Enamiku asutuste/ettevõtete jaoks muutuvad nende infosüsteemid aina olulisemateks ja missioonikriitilisemateks. Seega muutub üha tähtsamaks ka andmeturve, mis peab tagama infosüsteemide töövõimelisuse. Samal ajal muutub andmeturve järjest komplitseeritumaks ja ründed massilisemaks. Enam pole häkkimiseks vaja põhjalikke teadmisi - suvaline arvutiga ja Internetiühendusega koolipoiss on võimeline tekitama vägagi suuri probleeme, sest väga lihtne on Internetist leida häkkimiseks vajalikke teadmisi, konkreetseid ründekoode jms..

Käes on aeg kui iga firma, kellele infosüsteemi töösolek on oluline, peab andmeturbega tegelema ja teadma, mida selleks on vaja teha – st igal firmal peaks olema metoodika andmeturbeks vajalike meetmete/tegevuste määratlemiseks. Enam ei ole piisav (eriti rahvusvahelisel tasemel) kui öelda, et jah me tegeleme andmeturbega, kuid ei oska öelda (kirjas ka pole) mida, kuidas ja miks me täpsemalt teeme.

Jalgrataste leiutamise mõttetusest on tänapäeval üldiselt ka kõik teadlikud ja seega taandub küsimus järgimiseks sobiva metoodika valikule. On olemas päris mitmeid ja omade heade külgedega andmeturbe metoodikaid. Nende vahel valiku tegemiseks peame esmalt määratlema tegelikult vajatava/soovitava.

Andmeturbe üldmetoodikaid on kümneid ja ise sobiva otsimine võib osutuda küllaltki töömahukaks. Muidugi on kasulik olla kursis mitmetega, kuid enamasti peab arvestama ressursside (inimesed, aeg, raha) piiratuse ja majandusliku optimaalsuse tagamise nõuetega.

2.1. Sobiva andmeturbe metoodika valik

Veidi lihtsustatult võib andmeturbe üldmetoodikad jagada kaheks:

- andmeturbekesksed ja
- kontrolli/auditi kesksed.

Andmeturbekeskseid metoodikaid iseloomustab lähtumine vajalikest andmeturbe meetmetest/tegevustest – mida on vaja teha, et oleks tagatud infosüsteemi(de) turvalisus. Põhineb hetke parimale teadmisele/praktikale, vajab pidevat ajakohastamist, annab andmeturbe spetsialistile arusaadava ja üheselt mõistetava tegevuste loetelu.

Kontrollikesksed metoodikad põhinevad äriprotsesside ja nende turvariskide käsitlusel - määratletakse ohtude/riskide loetelu ja kontrollitakse kas kõigi nende jaoks on turvameetmed rakendatud ja piisavad (turvameetmete piisavuse hinnang sisuliselt põhineb ka hetke parimale teadmisele/praktikale). Kogu see riskide/ohtude temaatika on andmeturbe spetsialisti jaoks tore populaarteaduslik jutt, kuid sealt konkreetselt vajalikele andmeturbe meetmetele üleminek on tõeline peavalu - peab hakkama tekstist konkreetseid meetmeid välja otsima, need sobivalt grupeerima (lähtudes võimalikest realiseerimisvariantidest) jne.

Esmalt peakski endale andmeturbe metoodikat otsiv/valiv firma määratlema milleks tal seda vaja on – kas andmeturbe nõuetele vastavuse tõestamiseks (firma siseselt? teistele firmadele/asutustele? rahvusvaheliselt?) või andmeturbe süstemaatiliseks korraldamiseks (peamiselt vajalike turvameetmete määratlemiseks).

Muidugi on vägagi soovitav kasutada mõlemaid, sest koos nad täiendavad üksteist ja tagavad kindlamalt positiivse tulemuse (turvaintsidentide vähenemise/puudumise). Keerukate, kõrgete turvanõuetega ja missioonikriitiliste infosüsteemidega asutustele on kahe metoodika kasutamine lausa iseenestmõistetav – sisekontrolliks kontrollikeskne ja andmeturbeks andmeturbekeskne.

Kontrollikeskseid metoodikaid on andmeturbekesksetest tunduvalt rohkem. Ilmselt on kontroll/audit meeldivam tegevus- ja kirjutamisvaldkond.

Kontrolli/auditi keskseid andmeturbe metoodikaid:

- EVS-ISO/IEC 17799 Infotehnoloogia – Infoturbe halduse menetluskoodeks
- EVS-ISO/IEC 13335 Infotehnoloogia – Infoturbe halduse suunised
- ISO/DTR 13569 Infotehnoloogia – Pangandus ja sellega seotud rahandusteenused – Infoturbe suunised
+ Eesti riigi Andmekaitseinspektsioon
  Isikuandmete kaitse organisatsiooniliste ja tehniliste abinõude kirjelduse koostamise juhendmaterjal
- ISO 9000 series Quality Management standards
- COBIT (IT Governance Institute) + ISACA (Information Systems Audit and Control Association)
- Common Criteria (CC) for IT Security Evaluation (ISO/IEC 15408); Orange Booki, TCSEC-i ja ITSEC-i järglane.

Kui vajame metoodikat infosüsteemi rahvusvahelistele nõuetele vastavuse kontrolliks ja tõestamiseks, siis peaks valima mingi rahvusvaheliselt tuntud ja tunnustatud metoodika. Siin aga on probleemiks, et pole ülemaailmselt üldtunnustatut. Isegi Euroopa Liidu ulatuses mitte. Seega on hetkeseis selline, et kui on vaja oma andmeturbe tasemel olekut tõestada näiteks inglise firmale, siis oleks sobiv ISO 17799 (mis algselt oli British Standard 7799), saksa firmadega sobiks BSI metoodika, Ameerikas Common Criteria (vist). Tundub, et hetkel on sisuliselt parim, vägagi laialt kasutatav ning pidevalt ajakohastatav ja täiustatav COBIT. Päris ühest vastust küsimusele hetkel ei paista olevat.

Vajadusel saada andmeturve rahvusvaheliselt tunnustatult auditeeritud, on vägagi sobiv ja soliidne tellida see teenus väljastpoolt ja just sellele spetsialiseerunud rahvusvaheliselt tunnustatud firmalt ning nõutavale/sobivale kontrollimetoodikale vastavalt.

Kui andmeturbe teenust sisse ei osteta, siis andmeturbekeskne metoodika peaks ettevõttele kindlalt vajalik olema. Kusjuures andmeturbekeskne metoodika on ka täiesti sobiv ja piisav asutusesiseseks andmeturbe kontrolliks/auditiks.

Andmeturbekeskseid metoodikaid:

- Saksa Infoturbe Liiduamet (BSI)
  (Bundesamt für Sicherheit in der Informationstechnik - Federal Agency for Security in Information Technology) IT Baseline protection manual
  (on ka teisi etalonturbel põhinevaid metoodikaid, kuid BSI oma paistab olevat kõige põhjalikum ja pidevalt ajakohastatav)
- U.S. DEPARTMENT OF ENERGY Office of Security Affairs
  CLASSIFIED INFORMATION SYSTEMS SECURITY MANUAL
- Infosüsteemide Kolmeastmelise Etalonturbe Süsteem (ISKE) Rakendamisjuhend ver. 1.0 (RISO tellimusel Cybernetica AS)

Seega on valik küllaltki piiratud. Ka on vägagi küsitav nende otsese ülevõtmise otstarbekus.

BSI etalonturbe metoodika plussid/miinused:

+ BSI süsteem on väga põhjalik, detailselt dokumenteeritud ja teda täiendatakse regulaarselt kord aastas.
+ Etalonmeetmed võivad pakkuda ökonoomse lahenduse, sest samu või sarnaseid etalonmeetmeid saab suuremate pingutusteta kohaldada paljudele süsteemidele, kui suur hulk organsatsiooni süsteeme töötab ühises keskkonnas ja kui turbevajadused on võrreldavad.
+ Turvameetmete evitus nõuab riskianalüüsiks ja -halduseks ainult minimaalse hulga ressursse, seetõttu kulutatakse turvameetmete valimisele minimaalselt aega ja vaeva.
– Kui etalontase on seatud liiga kõrgeks, võib mõnede infotehnoloogiliste süsteemide turve olla ülemäära kõrgel tasemel (tähendab liigseid kulutusi).
– Kui tase on seatud liiga madalaks, võib mõnedel infotehnoloogilistel süsteemidel jääda turvet vajaka, nii et tulemuseks on kõrgem kaitsetuse tase.
– Missiooonikriitiliste ja kõrgete turvanõuetega infosüsteemide jaoks on etalonturbega majandusliku optimaalsuse tagamine praktiliselt võimatu - vajalikud turvameetmed võivad olla väga erinevad, isegi kui nõutav turvatase on sama.

USA Department of Energy astmelise metoodika plussid/miinused:

+ Väga hea on astmelisuse sissetoomine (erinevaid info turvanõuete klasse 54 ja neile vastavalt määratletud ka 54 vajalike turvameetmete komplekti) – saab just konkreetsele infosüsteemile konkreetselt vajalikud turvameetmed sõltuvalt turvanõuetest/turvaklassist ja sellega tagatud turvakulutuste majanduslik põhjendatus/optimaalsus.
+ Turvameetmete valimisele kulub minimaalselt aega ja ressursse (vajalik info ühe hiirekliki kaugusel).
– Infoturbenõuete klassifitseerimine mitte eriti õnnestunud – tavaline/üldlevinud kõrge-keskmine-madal (*high-middle-low*) (mingi asutuse keskmine võib olla teisele näiteks kõrge ja kolmandale hoopis madal).
– Ajakohastamisest infot pole (vähemalt pole see Internetis avalikustatud).

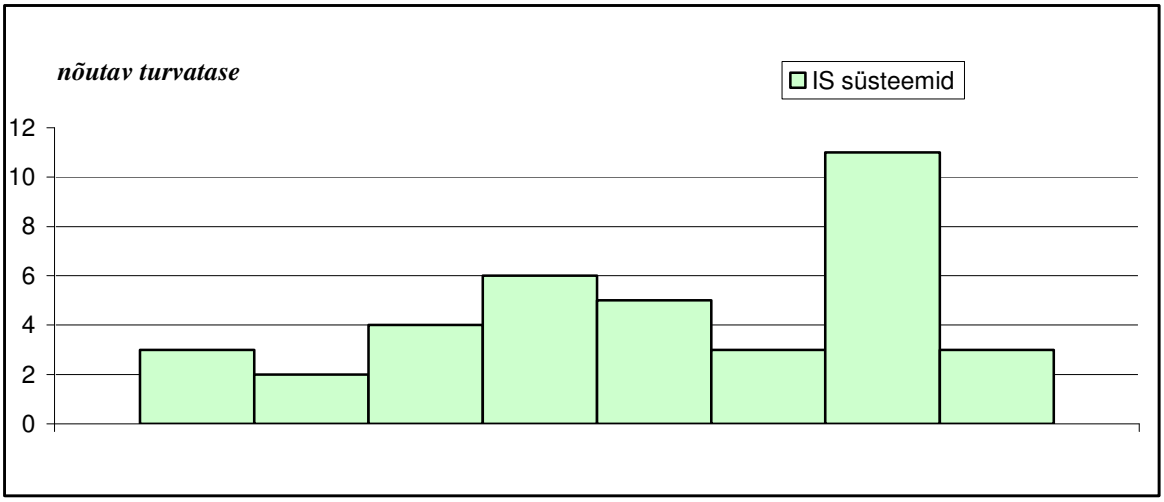
ISKE kolmeastmelise etalonturbe plussid/miinused:

+ Süsteem ISKE põhineb Saksamaa Infoturbeameti (Bundesamt für Sicherheit in der Informationstechnik, BSI) etalonturbe meetodikal ja käsiraamatul. Keskmine turbeaste M vastab täpselt BSI üheastmelisele süsteemile, mis on rajatud keskmise turbeastme saavutamiseks.
+ BSI süsteem on väga ulatuslikult ja detailselt dokumenteeritud ning teda täiendatakse regulaarselt kord aastas.
+ Kasutatakse Eesti Andmekaitse Inspektsiooni infoturbe nõuete klassifitseerimismetoodikat.
± Vajalike turvameetmete 3-ks astmeks jagamine on samm õiges suunas, kuid miks ainult 3-ks - elame ju infotehnoloogia ajastul ning pole oluline kas jagame 3-ks, 300-ks või 3000-ks astmeks – vajalik/soovitav info on ikka ühe hiirekliki kaugusel. Kui turvanõuetel on AKI metoodikas 256 astet, siis oleks otstarbekas kui nendele vastaks ka infoturbe (meetmekomplekside) 256 astet.
– Saksa keskmise riigiasutuse andmeturbele eraldatud ressursid on vähemalt suurusjärgu (küllaltki tõenäoliselt kahe) võrra suuremad kui eesti keskmisel riigiasutusel – peame kindlalt neist rohkem tähelepanu pöörama kulutuste põhjendatusele (kulutama just vastavalt info turvanõuetele ja väärtusele).

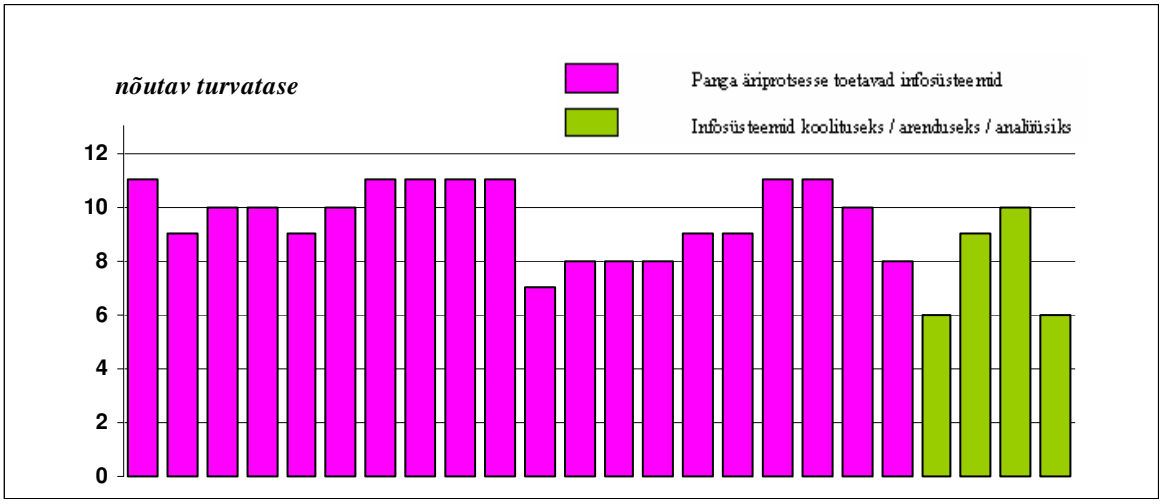
- Ühise kõrge taseme määratlemine suurima võimaliku turvataseme lähedale teeb majandusliku optimaalsuse tagamise praktiliselt võimatuks - vajalikud turvameetmed võivad olla väga erinevad, isegi kui nõutav turvatase on sama.
  Näiteks: IS1 S3 (nõuab krüptimist) K2 (tunnid)
  IS2 S2 (salajane) K3 (nõuab klustrit)
  (eeldatud on, et tagajärgede kaalukuse ja info tervikluse nõuded on mõlematel infosüsteemidel samad – näiteks "3")
  … ja IS1 pühul peaks kulutama miljoneid krüptolahendustele (ülisalajast infot peab ilmselt säilitama ainult krüpteeritult – krüpteeriv andmebaas vms, ka riistvarale erinõuded – infokandja varguse puhul info peaks hävinema jms) ning IS2-l hoopis klusterlahenduse tekitamisele.
- Internetis nähtud info põhjal tundub, et ISKE on tegelikult kolmeastmelise andmeturbe esimene täpsustamist ja ulatuslikku BSI juhendmaterjalide tõlkimist vajav algversioon.

Neljanda võimalusena võiks veel kaaluda ISO 13335 poolt soovitatud segametoodika kasutamist - esialgse jämeda riskianalüüsiga selgitada välja suurte riskidega (kõrgete turvanõuetega) ja asutuse tegevuse seisukohalt missioonikriitilised infosüsteemid ning neile teha vägagi töömahukas detailne riskianalüüs, kõigile teistele süsteemidele rakendada etalonturbe meetodit.

Segametoodika kasutamiseks sobiva asutuse integreeritud infosüsteemi nõutavate turvatasemete pilt oleks umbes järgmine (enamik infosüsteeme madalate/keskmiste ja ainult mõned kõrgete turvanõuetega):



Kuid samas vaatame joonist Ühispanga suhteliselt keerulise integreeritud infosüsteemi nõutavatest turvatasemetest:



Eesti Ühispanga (EÜP) Grupi äriprotsesse toetavate infosüsteemide (st tugeva enamiku) nõutavad turvatasemed on kõik küllaltki ühtlaselt kõrged – vahemikus 8 kuni 11. Arendus-, koolitus-, arhiivindus- ja analüüsisüsteemide nõutav turvatase on keskmine, kuid kahjuks moodustavad need süsteemid ainult umbes 10% infosüsteemidest.
Seega on pilt täiesti vastupidine segametoodikaks sobivale ja lootus riskianalüüsi traditsioonilise segametoodika rakendamise otstarbekusest Ühispangas ei pea paika, sest:
• detailne riskianalüüs tuleks korraldada kõigile põhilisi äriprotsesse toetavatele infosüsteemidele ning see kujuneks vägagi töö- ja ajamahukaks;
• etalontaseme määratlemine suurima võimaliku turvataseme lähedale teeb majandusliku optimaalsuse tagamise võimatuks - vajalikud turvameetmed võivad olla väga erinevad, isegi kui nõutav turvatase on sama.

Andmeturbe metoodika valiku kokkuvõtteks:

- **esimene ja väga oluline samm on määratleda millist metoodikat vajatakse – andmeturbekeskset või kontrollikeskset;**
- **kui ettevõte piirdub ühe andmeturbe metoodikaga, siis peaks see olema üldjuhul andmeturbekeskne (sobib ka asutuse siseks kontrolliks);**
- **andmeturbekeskseid metoodikaid on vähe ning kõrgete turvanõuetega ja missioonikriitilistele infosüsteemidele (varsti on see ilmselt nii enamustel ettevõtetel/asutustel) rakendamiseks sobivat tegelikult polegi.**

Seega - kätte on jõudmas (jõudnud?) aeg ja vajadus infoturbe uue mudeli jaoks.

Andmeturbekeskse metoodika puhul on tegelikult ainult kaks valikuvarianti:

1. kui majanduslik optimaalsus pole eriti oluline, siis etalonturve

või

2. kui loeme majandusliku optimaalsuse oluliseks, siis tuleks valida astmeline metoodika ning selleks on algseid valikuvariante on ilmselt jälle kaks:
   - ISKE

   või
   - käesolevas töös edaspidi detailsemalt käsitletav astmeline metoodika.

Veidi ette rutates (kuid, et olulised tegevused/nende järgnevused saaksid ühes kohas üles loetletud) – mingi olemasoleva astmelise metoodika Eesti riigiasutustele sobivaks kujundamisel on järgmisena vajalik infoturbenõuete klassifitseerimismetoodika täpsustamine/ajakohastamine (praegune ilmselt vajab seda – vt 3.1.).
Etalonturbe puhul info turvanõuete klassifitseerimisega ja selle ajakohastamisega tegelemine pole vajalik - nõutavad turvameetmed ju sisuliselt turvanõuetest ei sõltu.

3. ASTMELINE ETALONTURVE

Ühispangale sobiva vajalike infoturvameetmete määratlemiseks sobiva metoodika puudumisest tingitult oleme Eesti Ühispangas välja töötanud astmelise etalonturbe metoodika (samas võiks see olla ka üheks täiesti arvestatavaks alternatiiviks suvalisele firmale Eestis, kes otsib endale metoodikat andmeturbe korraldamiseks).

Astmelise etalonturbe põhieesmärgiks on välja pakkuda asutuste/ettevõtete infosüsteemidele turvariskide maandamiseks vajalike turvameetmete määratlemiseks metoodika, mille teostamiseks kulub minimaalselt ressursse (st töömaht oleks ligikaudu sama, mis etalonturbe puhul) ja mis tagab igale infosüsteemile konkreetselt vajaliku/nõutava turvanõuete taseme (st turvanõuete igale astmele määratletakse vastavad vajalikud turvameetmed).

Jalgrattaid me leiutama ei hakanud, ühendasime kaks head ideed:

- Eesti Andmekaitse Inspektsiooni klassifitseerimismetoodika
- USA Energeetikaministeeriumi turvaklassist lähtuv turvameetmete määramise astmeline metoodika (graded security requirements -> graded security measures complexes).

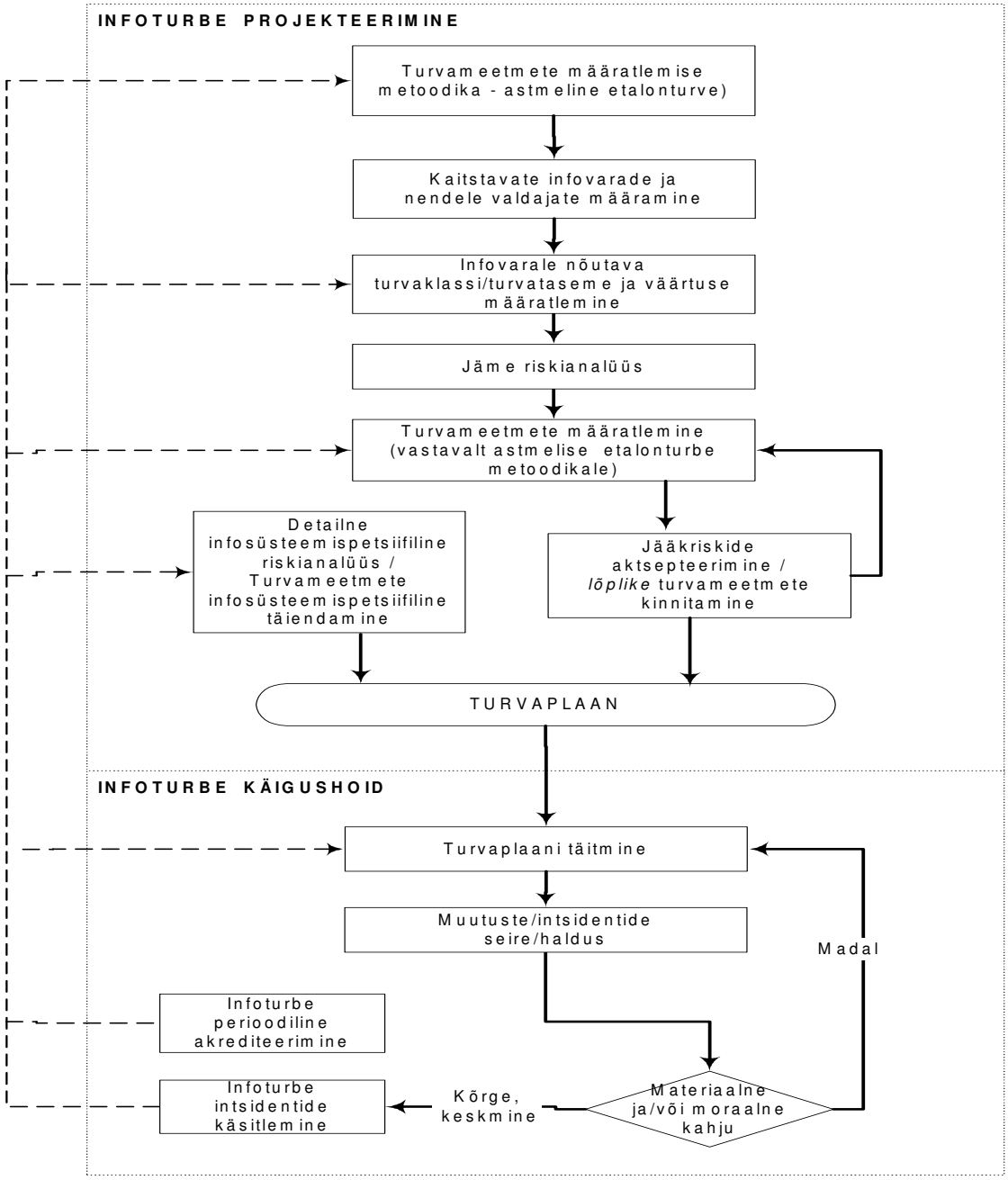
Astmeline metoodika põhineb seega seni USA Department of Energy mitmete infosüsteemide detailsete riskianalüüside üldistusel ja muidugi ka kogu infoturbealase tegevuse (Eestis Ühispanga ja Politseiameti) eelneval kogemusel.

Astmelise etalonturbe metoodika on etalonturbe metoodika edasiarendus, kus ISde turvanõuded (konfidentsiaalsusele, käideldavusele, terviklusele) jagatakse astmeteks (tasemeteks 0 kuni 3)) ning on loetletud vajalikud turvameetmed (4+4+4+4=16 komplekti) turvanõuete kõigi astmete (4x4x4x4=256 astet) tagamiseks, st määratakse turvanõuete vajalikele astmetele vastavad etalonastmed.

Klassifitseerimisel kasutatav hilinemise tagajärgede kaalukuse praeguse tõlgenduse põhjal ei teki sealt eriti otseseid seoseid turvameetmete määratlemisega. Seosed esinevad ilmselt ainult talitluspidevusega seonduvalt. Turvameetmete algvaliku mätta otsast vaadates on seega pigem tegemist 12-ne (4+4+4) erineva turvaklasside komponendiga ja nende baasil on võimalik moodustada 64 (4x4x4) erinevat turvaklassi. Võimalik, et 64 ongi täiesti piisav astmelisuse tase (?).

Riskianalüüs astmelises etalonturbes (vt Joonis 1):

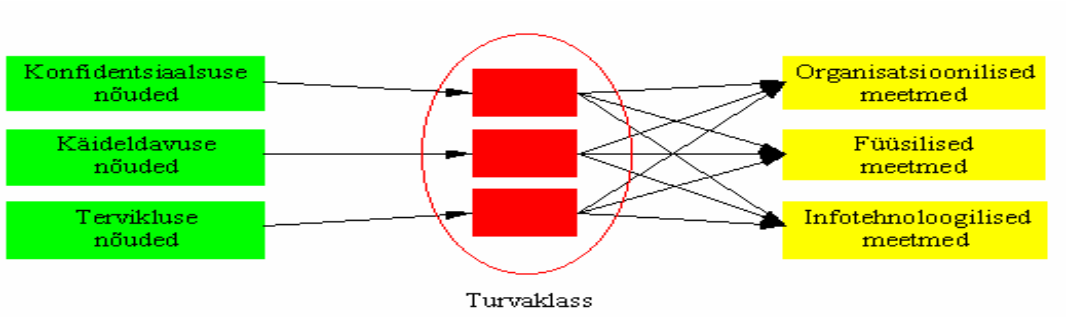
- tuleb kindlaks teha infosüsteemi võimalik kuuluvus mingisse erikategooriasse (st süsteemi võib adekvaatselt turvata ka ilma astmeliste turbemeetmeteta) ja/või lepingutest/seadustest jms tingitud spetsiifiliste erinõuete olemasolu ning sellest tulenevad vajalikud/lisanduvad turbemeetmed
- kõigile infosüsteemidele esialgseks (kiiret realiseeritavust tagavaks) infoturbe meetmete määramiseks kasutatakse astmelist turvameetmete määramise metoodikat,
- edasist turvaanalüüsi viiakse läbi kasutades selleks põhiliselt turvaintsidentide seire/analüüsi tulemusi (st. lähtutakse hetkeolukorrast ja minevikust lähtuvast infost), mille põhjal vajadusel kas muudetakse/täiendatakse astmeliste turvameetmete metoodikat või (kui intsident on tõesti infosüsteemispetsiifiline) töötatakse välja konkreetsed lahendus(ed) konkreetsele infosüsteemile kasutades selleks detailset riskianalüüsi metoodikat,
- toimub nii ettevõtte (integreeritud) infosüsteemi kui ka infotehnoloogia üldisest arengust tingitud perioodiline infoturbe metoodika kontroll/ajakohastamine.



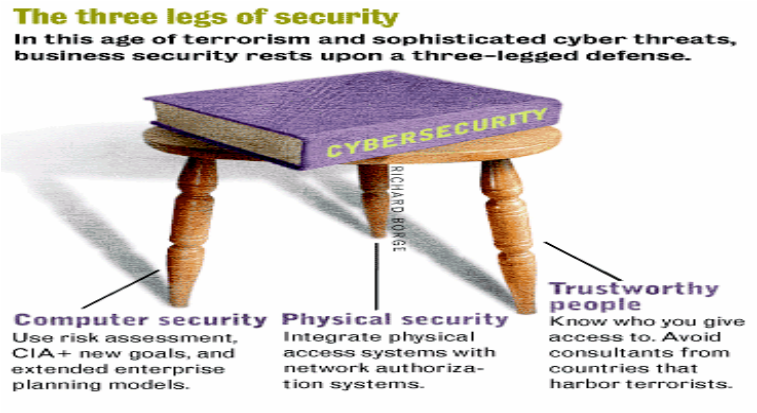
Joonis 1. Infoturbe meetmete määramine

Eduka realiseeritavuse tagamiseks on oluline vajalikud turvameetmed loogiliselt grupeerida.

Andmeturbe tegevusvaldkondadest rääkides on küllaltki levinud hüüdlause, et infoturve püsib kolmel sambal (n Eesti Andmekaitse Inspektsiooni ettekujutusest Joonis 2 - organisatsioonilised-, füüsilised ja infotehnoloogilised meetmed), kuid eri käsitlustes kipuvad need kolm sammast erinevad olema (vt ka Joonis 3).



Joonis 2. Turvanõuded -> Turvaklass -> Turvameetmed



Joonis 3. Infoturbe kolm sammast.

Viimasel ajal kasutatakse üldiselt veidi detailsemat põhisammaste ning vastavate tegevusvaldkondade jaotust :
- PERSONAL
- INFRASTRUKTUUR
- TURVAORGANISATSIOON
- INFOTEHNOLOOGILISED VAHENDID JA NENDEGA OTSESELT SEOTUD MEETMED
- TALITLUSPIDEVUS

Väga oluline on ka tegevusvaldkondade sisene turvategevuste loogiline jaotus/grupeerimine. Allteemadeks jaotamisel on lähtutud kahest põhimõttest :

- kõik tegevusvaldkondade eriti olulised turvategevused peaksid olema vastava allteemana välja toodud,
- allteemana välja toodud turvameetmete-gruppi peaks üldjuhul saama ellu viia ühe rakenduse või rakendus(t)e kompleksiga ja soovitavalt peaks see kuuluma IT ühe struktuuriüksuse (spetsialisti) teadmiste- ja tegevusvaldkonda - st on arvestatud, et vajalike turvameetmete-grupi realiseerimiseks oleks olemas sobivad tehnilised ja infotehnoloogilised lahendused.

Käsitlemise loogikast lähtudes on turvameetmed jagatud kahte gruppi:

1) üldkohalduvad turvameetmed - ei sõltu töödeldava informatsiooni turvaklassist;
2) astmelised turvameetmed - sõltuvad töödeldava informatsiooni turvaklassist).

Eelnevate põhimõtete järgimisel saime astmeliseks etalonturbeks vajalike turvameetmete (kokku on neid metoodika hetkeversioonis ~450) järgneva jaotuse/grupeeringu:

ÜLDKOHALDUVAD TURVAMEETMED :

TURVAORGANISATSIOON
1. Infoturbe poliitika ja strateegia määratlemine ning organisatsiooni loomine
2. Infovarade kindlaksmääramine
3. Infovarade valdamine (valdamiskord, valdajate määramine), infovaradele turvanõuete määramine ja infovarade klassifitseerimine
4. Infoturbe meetmete määratlemine (metoodika, kord)

VÕIMALIKUD ERINÕUDED INFOSÜSTEEMILE
5. Kuuluvus erikategooriasse
6. Nõuded, mis tulenevad:
   1) seadustest, standarditest, eeskirjadest või
   2) lepingutest kolmandate osapooltega.

ASTMELISED TURVAMEETMED :

TURVAORGANISATSIOON
1. Turvadokumentatsiooni ja muudatuste haldus (DOK)
2. IS turbe akrediteerimine (TA)

PERSONAL
3. IT personalihaldus (ITP)
4. Töötajate instrueerimine, koolitus ja atesteerimine (IKA)

INFRASTRUKTUUR
5. Füüsiline turve (FT)
6. IS kasutajate tööruumid (TRM)
7. Spetsiaalruumid (serveri- ja sideruumid) (SRM)

INFOTEHNOLOOGILISED VAHENDID
8. Pääsuõigused (PÕ)
9. Side (KOM)
10. Välisperimeetri kaitse (VPK)
11. Sisevõrgu turve (SVT)
12. Viiruste ja õelkoodi tuvastamine ning tõrje (VÕT)
13. Info krüpteerimine (KR)
14. Seire, analüüs (MON)
15. IS kasutajate töö jälgimine (KJ)
16. Andmete varundamine ning taastamine (AVT)
17. IS hooldus (ISH)
18. Infoturvaintsidentide haldus (TIH)
19. IS sisseostmine ja arendus (ISA)
20. IS testimine (IST)
21. Ajakohastamine, kontroll ja turvatestimine (AKT)

TALITLUSPIDEVUS
22. Talitluspidevuse ja taasteplaanid (TTP)
23. Infosüsteemide taasteplaanid (ISTP)

Vajalike infoturbe meetmete määratlemine:

- Teeme kindlaks erinõuetest tulenevad vajalikud turvameetmed, mis:

  infosüsteemi kuulumisel mingisse erikategoorisse (spetsiaalsüsteemid, mida võib adekvaatselt turvata ka ilma astmeliste turvameetmeteta) välistavad vajaduse järgnevaks astmeliste turvameetmete määramiseks

  või

  lisanduvad järgnevalt määratletavatele astmelistele.

- Turvatava informatsiooni turvanõuded ning turvaklassifikaatorid määravad vajalikud astmelised turvameetmed (vt Tabel 1. Astmeliste turvameetmete määramine lähtuvalt nõutavast turvaklassist.)
- Vajalikud astmelised turvameetmed koos võimalike erinõuetest lisanduvate meetmetega määravadki turvatavat infot töötleva infosüsteemi turvamiseks vajalikud turvameetmed.

Eelkirjeldatud turvameetmete loetelu on järgneva analüüsi (turvameetmete majanduslik otstarbekus, riskide aktsepteerimise) etapi aluseks (vt Joonis 2. Infoturbe meetmete määramine).

Astmelise etalonturbe plussid:

* Turvanõuete igale komplektile, st igale turvaklassile, seatakse vastavusse just sellele klassile sobiv ja vajalik turvameetmete komplekt.
AKI klassifitseerimismetoodika järgi on infosüsteemidele võimalik moodustada 16-ne (4+4+4+4) erineva turvaklasside komponendi baasil 256 (4x4x4x4) erinevat turvaklassi. Seejuures määratleb astmeline etalonturve 256 etalontaset, st 256 erinevat *turvameetmete komplekti.*

* Igale infosüsteemile saab kiiresti ja optimaalselt määratleda konkreetsed vajalikud ja nõutavad turvameetmed – vajalik info on ühe hiirekliki kaugusel.

* Lõpptulemusena saadakse turvameetmete loetelu (tegevusvaldkondade ning allteemade kaupa), mida pole vaja nuputada või välja otsida populaarteaduslikest tekstidest.

* Infoturbemeetmed on valdkonniti loogiliselt ja edaspidist realiseerimist silmas pidades rühmitatud allteemadeks.

* Võimaldab ja ühtlasi tagab ka juba turvatud infosüsteemide infoturbe kiire ning optimaalse kontrolli – kas kõik vastaval astmel nõutavad turvameetmed on ka tegelikult realiseeritud.

* Võimaldab infosüsteemide turvaanalüüsil ja jääkriskide aktsepteerimisel täpselt määratleda kõik mittevajalikuks osutuvad turvameetmed.
Aktsepteerides mingit konkreetset jääkriski (sisuliselt aktsepteerides soovitavatest erinevaid turvanõudeid) muutub sisuliselt ju ka infosüsteemi turvaklass ja sellele vastav etalontase. Kõiki ebavajalikeks jäävaid turvameetmed on väga lihtne piiritleda erinevate etalontasemete meetmete erinevusena ja ühe mitteotstarbekaks tunnistatud/aktsepteeritud turvameetme asemel saame neid enamasti mitu.

* Kui otsustatakse kasutada etalonturvet, siis võimaldab astmeline etalonturve kiiresti määratleda just konkreetse(te)l etalontaseme(te)l vajalikud turvameetmed.

* Kui otsustatakse kasutada detailset süsteemianalüüsi, siis võimaldab astmeline etalonturve kiiresti kontrollida detailse analüüsiga saadud turvameetmete loetelu – kiiresti saab kindlustunde suuremate vigade puudumisest (ka rätsepaülikond võib vahel ebaõnnestuda).

Astmelise etalonturbe praeguse versiooni on välja töötanud Eesti Ühispanga andmeturbegrupp ning see on juurutatud ka Eesti Haigekassas ja Eesti Politseiametis. Vaja oleks andmeturbespetsialistide laialdasemat koostööd, et tagada metoodika laialdasem sobivus erinevatele asutustele. Algatuse selliseks koostööks on teinud Riigi Infosüsteemide Arenduskeskus (RIA):

http://www.ria.ee/dirs/standardisation/evstk4_deliberations.html?id=39 ja
http://www.ria.ee/dirs/standardisation/Astm_etalonturbe_juhend.doc.

Konkreetsele infosüsteemile turvameetmete määratlemine jaotub sisuliselt kolmeks alamülesandeks:

- **turvanõuete püstitamine (st saame vajaliku/nõutava turvaklassi)**
- **vajalike turvameetmete algvalik (määratlemine lähtudes vajalikust/nõutavast turvaklassist)**
- **infosüsteemile sobivate turvameetmete (teatud ajaks) *lõplik* valik (analüüs, jääkriskide aktsepteerimine)**

3.1. Info turvanõuete ja väärtuse määratlemine - st info klassifitseerimine

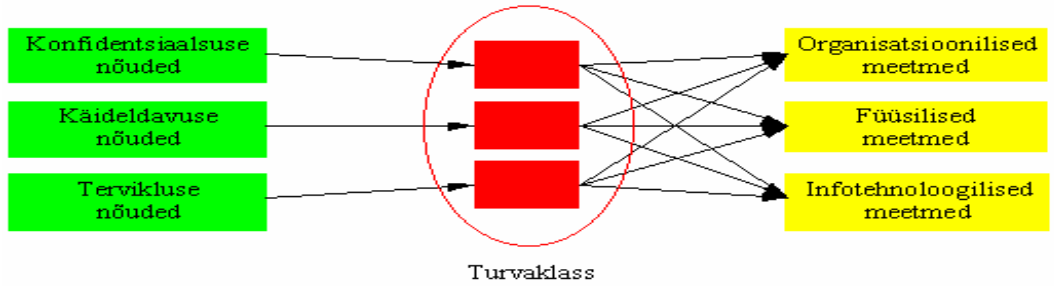
Klassifitseerimise eesmärk on jaotada asutuse halduses olevad infovarad turvaklassidesse, et järgnevalt määrata nende turvaklassidele vastavad turvameetmed.

Infosüsteemile vajalike turvameetmete valimine toimub turvavajadustest lähtuvalt määratletud turvanõuetest/turvaklassist. Turvavajaduse väljaselgitamisel ja turvanõuete püstitamisel on aluseks infovaradele valdaja/omaniku poolt antud hinnangud, ohu- ja riski-analüüsi tulemused ja ka kehtivatest andmeturvet puudutavatest seadustest/eeskirjadest/lepingutest tulenevad nõuded.

Turvaklassid on nii turvanõuete kui ka -meetmete komplekside sümbolid, mis ei sõltu turvavajaduste põhjustest.
Turvaklass omistatakse üldjuhul kogu andmebaasile/andmekogule/infofailile, kuid vajadusel ka selle osale, üksikutele andmeväljadele või ka teatud päringutele.

Eestis kujunenud praktika kohaselt seisneb infoturbe nõuete ja vastava turvaklassi määratlemine selles, et konkreetsele infole ja seda töötlevale infosüsteemile omistatakse nii konfidentsiaalsus-, käideldavus- (aegkriitilisus ja hilinemise tagajärgede kaalukus) kui ka terviklusnõuded.

Turvanõuded -> Turvaklass -> Turvameetmed:



Turvaklassi võib äriinfo valdaja seisukohalt vaadelda kui turvanõuete komplekse. Turvaspetsialisti seisukohalt võib turvaklassi vaadelda kui turvameetmete kompleksi, mis ei sõltu turvavajaduse põhjustest.
Eestis kujunenud praktika ning andmekaitseinspektsiooni kehtestatud üldpõhimõtete alusel peetakse riigiasutuste jaoks infoturbenõuete ja turvaklasside määramisel-kehtestamisel silmas allpool esitatud eesmärke ja tingimusi.

Konfidentsiaalsuse alusel määratavad andmeturbenõuded ning vastav klassijaotus on järgmised:
S0 – teabele ei ole seatud mingeid juurdepääsupiiranguid

S1 – teabele juurdepääs on lubatud ainult teatud tingimuste täitmisel
S2 – teabele juurdepääs on lubatud ainult subjektil, kelle kohta töödeldav teave käib, või infosüsteemi omaniku nõusolekul
S3 – teave on seaduses või seaduse alusel salastatud

Teabe aegkriitilisuse alusel määratavad andmeturbenõuded ning vastav klassijaotus on järgmised:
K0 – teabe saamisele ei ole seatud tähtaegu
K1 – teabe saamisele on seatud tähtaeg päevades
K2 – teabe saamine on oluline tundide jooksul
K3 – teabe saamine on oluline sekundite jooksul

Teabe hilinemise tagajärgede alusel määratavad andmeturbenõuded ning vastav klassijaotus on järgmised:
R0 – teabe mittesaamisega ei kaasne tagajärgi
R1 – teabe mittesaamine võib takistada funktsiooni täitmist
R2 – teabe mittesaamine toob kaasa olulise takistuse funktsiooni täitmisel
R3 – teabe mittesaamine toob kaasa funktsiooni mittetäitmise

Teabe tervikluse alusel määratavad andmeturbenõuded ning vastav klassijaotus on järgmised:
T0 – teabe allikas ega muutmise tuvastatavus ei ole olulised
T1 – teabe muutmine peab olema tuvastatav
T2 – teabe allikas peab olema tuvastatav
T3 – teabel on tõestusväärtus (st ka juriidiline)

Mõned aastad tagasi kehtinud klassifitseerimismetoodika sisaldas ka info väärtust (st hilinemise tagajärgede kaalukus oli siis rahas mõõdetav/määratav).
Siis oli hilinemise tagajärgede kaalukus:
R0 – andmete õigeaegne mittesaamine ei too kaasa mainimisväärseid tagajärgi
R1 – andmete õigeaegne mittesaamine põhjustab häireid asutuse tegevuses, ohtu inimeste tervisele või keskkonnasaaste ohtu ja/või sadadesse tuhandetesse kroonidesse ulatuvaid kahjusid
R2 – andmed, mille õigeaegne mittesaamine põhjustab olulist kahju asutuse mainele, ohtu inimelule või keskkonnasaastet ja/või miljonitesse kroonidesse ulatuvaid kahjusid
R3 – andmete õigeaegne mittesaamine põhjustab asutuse pankroti, kahju, mis on võrreldav ettevõtte aastakäibega, mitmeid hukkunuid või ulatuslikku keskkonnasaastet ja/või kümnetesse miljonitesse ulatuvaid kahjusid

Eesti riigi (Andmekaitse Inspektsiooni) info klassifitseerimismetoodika töötati välja aastatel 1997 ja 1998 ning oli selle aja kohta kõrgel tasemel. Eriti hea oli lähenemine alamteemade astendamisele – mitte tavaline/üldlevinud kõrge-keskmine-madal (*high-middle-low*) (mingi asutuse keskmine võib olla teisele näiteks kõrge ja kolmandale hoopis madal), vaid kõigile asutustele/ettevõtetele üheselt mõistetav/mõõdetav.

Aeg on edasi läinud, kuid klassifitseerimismetoodika paraku mitte. Praktikas on ilmnenud ajakohastamist/täiustamist vajavaid kohti:
– Infoturbe mõttekate kulutuste piiritlemisel on väga oluline info väärtus (varasem metoodika sisaldas seda). Äriinfo väärtus sisuliselt fikseeriks maksimaalsed mõttekad kulutused infoturbele.
– Info tervikluse käsitlusest on välja jäänud selle õigsus/täielikkus (praeguses on sisuliselt ainult tuvastatavus). Kuid küllalt tihti (nt eelkõige panganduses) võib info õigsuse/täielikkuse puudumine põhjustada suuremaid kahjusid, kui on võimalik hiljem tuvastatavusega tagasi saada.

– Käideldavuse juures (eelkõige teabe saamist sekundite jooksul nõudes) tuleks ikkagi arvestada ka töökindluse nõudeid. Teabe saamist alati sekundite jooksul nõudes on ainuvõimalikud infosüsteemide klasterlahendused, kuid näiteks 99,9% töökindlust lubades võib nädalas olla üks kuni kümneminutiline infosüsteemi seisak ja piisavaks võivad osutuda dubleerivad/replitseerivad lahendused – rahalised kulutused erinevad aga ligikaudu suurusjärgu võrra.
Veel on väga oluline, kas käideldavuse nõuded peavad olema tagatud 7 × 24 või 5 × 8 tundi nädalas (praktikas kaks väga levinud varianti).

Vaja oleks klassifitseerimisel arvesse võtta info väärtust, mida esimeses lähenduses võiks määratleda kui nõutava turvataseme mittetagamisel vastava funktsiooni (korrektsest) mittetäitmisest tingitud võimalikud kahjud (saamata jäävad tulud, võimalikud leppetrahvid jms). Lõplikul/täpsemal infovara väärtuse määratlemisel lisanduvad veel kulutused taastamisele. Info väärtus on hädavajalik turvameetmete realiseerimise majandusliku otstarbekuse hindamise ja jääkriskide aktsepteerimise etapil. Varasem hilinemise tagajärgede kaalukuse (R) ka rahas väljendamine oli ilmselt parem. Äriettevõttele ei valmista erilist raskust oma äriinfo rahalise väärtuse määratlemine, riigiasutustele on see millegipärast tihti tõsine probleem.

Praegune tagajärgede kaalukuse tõlgendus tekitab väga vähe otseseid seoseid turvameetmete määratlemisega (seosed praktiliselt ainult talitluspidevuse - ja taasteplaanide osas). Ehk oleks siia mõttekas asemele tuua infosüsteemi missioonikriitilisuse mõiste - kui infosüsteem ei tööta, siis võib öelda, et ka asutus praktiliselt (näiteks ~80%) ei tööta + kõrged turvanõuded + suured potentsiaalsed kahjud.

Riigiasutused (kuid tegelikult igasugune asutus, kellel on tegemist delikaatsete ja eraeluliste isikuandmetega) peavad järgima AKI klassifitseerimismetoodikat, kuid see ei keela ka praegu tegemast rohkem kui nõutud, st kasutada võib ka veidi keerukamat metoodikat.

3.2. Vajalike infoturbe meetmete määratlemine

Turvatavat infot töötleva infosüsteemi turvamiseks vajalikud turvameetmed saame kui seadustest/eeskirjadest/lepingutest ning erinõuetest tulenevatele turvameetmetele lisame järgnevalt määratletavad astmelised (mõningaid nn *erisüsteeme* võib adekvaatselt turvata isegi ilma astmeliste turbemeetmeteta).

Astmelised turvameetmed määrame valdaja poolt turvatavale infole esitatud turvanõuetele vastavalt (vt Tabel 1. Astmeline turvameetmete määratlemine):

- Määrame tabelis edasise töö aluseks olevad veerud vastavalt turvatava informatsiooni turvanõuetele/turvaklassifikaatoritele.

- Leiame tabelis valitud veergudest kõigile ridadele astme maksimumi reas - tulemus tabeli viimasesse veergu (vt Tabel 1 – veerg **"**Vajalikud meetmete astmed - nõutavatele turvaklassifikaatoritele vastavalt meetme maksimaalne aste reas") – sisuliselt leidsime vajalikud meetmete astmed turvatavat infot töötleva infosüsteemi kõigile infotöötlusressurssidele / -protsessidele.

Vajalikele astmetele vastavad turvameetmete loetelud saame tabeli 1 esimeses veerus toodud sisukorrapunkti alt.

Vajalike turvameetmete summaarne loetelu (seadustest/eeskirjadest/lepingutest/erinõuetest tulenevad + astmelised) on järgneva analüüsi (turvameetmete majanduslik otstarbekus, riskide aktsepteerimise, *lõplikud* turvameetmed) etapi aluseks.

3.3. Infosüsteemile sobivate turvameetmete (teatud ajaks) lõplik valik

Sisuliselt on tegemist eelnevate teemade praktilise teostamisega – kõigile infosüsteemidele määrata soovitavad infoturvanõuded ja info väärtused ning valitud turvameetmete määratlemise metoodikat järgides ka vajalikud turvameetmed.

Lisandub jääkriskide aktsepteerimise ja turvameetmete lõplik valimine.

Turvameetmete lõpliku valimise protsess jaguneb sisuliselt kaheks etapiks:

- analüüs: hinnatakse infosüsteemile turvameetmete spetsifitseerimise protsessi tulemusena saadud turvameetmete majanduslikku otstarbekust (või olemasolevate sobivust/otstarbekust). Infovarade kaitse peab olema tagatud kasutades parimaid ning ühtlasi majanduslikult mõttekaid/optimaalseid turvameetmeid (st peab olema tagatud majanduslik tasakaal turvariskidest tingitud võimalike kahjude ja turvakulutuste vahel);
- turvameetmete lõpliku komplekti valimine/määramine: eelnenud analüüsi tulemuste põhjal tehakse otsus jääkriskide aktsepteerimiseks või mitteaktsepteerimiseks (kulutuste majanduslikust otstarbekusest) ja kinnitatakse infovarale lõplik turvaklass/turvameetmed.

Ettevõtte infosüsteemi muudatustest ja infotehnoloogia üldisest arengust tingituna tuleb infovarade ja vajalike turvameetmete nimistut pidevalt ajakohastada. Eelnevast tuleneb ka vajadus infovarade klassifitseerimise/ümberklassifitseerimise ajakohastamiseks.
Ümberklassifitseerimine võib osutuda vajalikuks ka turvameetmete analüüsi / lõpliku määramise protsessis – näiteks kui osutub majanduslikult või tehniliselt otstarbekaks aktsepteerida jääkriske.

4. ASTMELISE ETALONTURBE JUHENDMATERJAL ver. 2

Käesolev dokument käsitleb asutuse ja selle allasutustes infosüsteemidele infoturbe meetmete määratlemist lähtudes informatsiooni valdaja poolt esitatud turvanõuetest/turvaklassist.

Juhendi koostamisel on lähtutud:
- standardis ISO 17799 esitatud põhimõtetest/nõudeist,
- USA Energeetikaministeeriumi "Astmeliste infoturbe meetmete määramise metoodika",
- Eesti riigi infosüsteemide turvaalase klassifitseerimise üldpõhimõtetest,
- Ühispanga infoturbe astmelise metoodika 2000. a. versioonist,
- kogemustest astmelise infoturbe metoodika juurutamiselt Eesti Haigekassas ja Eesti Politseiametis.

Põhieesmärgiks on saada asutuse (ja tema allasutuste) jaoks optimaalne (aeg, raha) infosüsteemidele turvariskide maandamiseks vajalike meetmete määramise juhend, mis tagaks infovara omaniku poolt nõutava turvanõuete (aktsepteeritud turvanõuete/aktsepteeritud jääkriskide) taseme.

Käesoleva versiooni 2 tegemise konkreetsemateks eesmärkideks on:
- ajakohastada metoodika 2000.a. versioon,
- kontrollida Eesti Ühispanga astmelise etalonturbe turvajuhendi vastavust ISO 17799 standardiga.

Tänud praktikandile IT kolledžist Helena Tiimusele ja tema suurepärasele diplomitööle „Turvakontseptsioonid: andmeturbekeskne versus kontrolli- ja auditipõhine" – meie koostöös valmis kokkuvõtlik loetelu Eesti Ühispanga turvajuhendisse ISO 17799'ga vastavuse tagamiseks lisamist vajavatest turvameetmetest. Töö käigus sai selgeks, et ISO 17799 vajaks ka ise ajakohastamist, kuid see on juba teiste tegijate mängumaa.

Põhjused miks ISO 17799's nõutud turvameede puudus EÜP Astmelise infoturbe metoodikas (kokku saime neid ~50):
- olid teistes EÜP infoturbe kordades juba varem kirjeldatud,
- olid juba kirjeldatud EÜP füüsilise turbe kordades (Ühispangas on infoturbeks ja füüsiliseks turbeks eraldi struktuuriüksused),
- puudusid EÜP's iseenesestmõistetavateks peetud punktid,
- tegelikult/sisuliselt puuduvad – st pole astmelises metoodikas ega ka teistes EÜP kordades, kuid peaksid olema.

Käesolev astmelise etalonturbe metoodika realisatsioon pole mingi *lõplik* tõde - vajalik on selle pidev/perioodiline üldistamine, täpsustamine ja ajakohastamine. Ei maksa loota sellise üldmetoodika 100%-sele täpsusele/üldsobivusele. Oluline oleks turvameetmete määratlemiseks metoodika olemasolu, mis annaks infosüsteemi turvanõuetele/turvaklassile vastava/põhineva algversiooni vajalikest turvameetmetest ja näiteks ˇ90%-ne täpsus oleks täiesti hea ning piisav. Nagu senine kogemus näitab tuleb arvestada konkreetsete infosüsteemi- ja asutusespetsiifiliste täpsustustega ligikaudu ±5%.

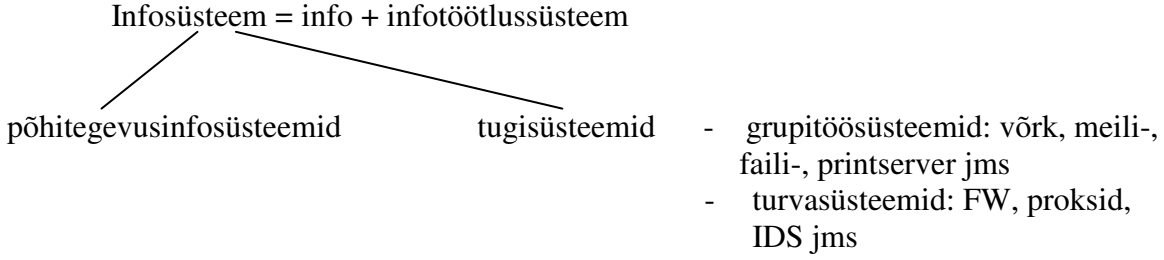
MÕISTED ja SELGITUSED

- **IT juht** – asutuse või selle allasutuses IT eest vastutav isik
- **Andmeturbejuht** – asutuse või selle allasutuses andmeturbe eest vastutav isik
- **IT hooldusjuht** – asutuse või selle allasutuses infosüsteemide hoolduse eest vastutav isik

- **IT arendusjuht** – asutuse või selle allasutuses IT arenduse eest vastutav isik
- **IT juhtkond** – koosneb IT juhist, andmeturbe juhist, hooldusjuhist ja arendusjuhist
- **kriisijuht** - asutuse juht või tema poolt määratud/volitatud kriisisituatsioonide lahendamist juhtiv/koordineeriv isik
- **Etalonturbe metoodika -** kui rakendame teatud loetletud turvameetmed, siis on keskmise (riigi)asutuse jaoks turvariskid maandatud. Põhineb mingi tunnustatud organisatsiooni, näiteks Bundesamt für Sicherheit in der Informationstechnik – Saksamaa Infoturbe Liiduamet,eelnevatel kogemustel ja/või teostatud riskianalüüsil.
- **Astmeliste turvameetmete metoodika -** etalonturbe metoodika edasiarendus, infosüsteemide turvanõuded (konfidentsiaalsusele, käideldavusele, terviklusele) jagatakse astmeteks (tasemeteks 0 kuni 3)) ning on loetletud vajalikud turvameetmed turvanõuete kõigi astmete tagamiseks – st määratakse turvanõuete vajalikele astmetele vastavad vajalikud turvameetmed ja nende astmed. Turvanõuded esitavad süsteemile info valdajad ning määravad sellega infosüsteemi turvaklassi, mis omakorda määrab vastava infosüsteemi infoturbeks vajalike turvameetmete kompleksi. Saadud vajalike turvameetmete kompleks tagab, et asutuse jaoks on turvariskid majanduslikult optimaalselt maandatud.
- **Turbe tugisüsteemid -** infosüsteemid (riistvara, tarkvara ja kommunikatsioonid - näiteks tulemüürid, Kerberos autentimiseks/autoriseerimiseks, VPN, SSA, logimis- ja jälgimissüsteemid, turvaanalüüsisüsteemid), mis on vajalikud põhitegevusprotsesside toimimist tagavate infosüsteemi(de) infoturbe tagamiseks. Seega on turvameede muutunud infosüsteemiks, mida on omakorda vaja turvata.
- **SANEERIMINE -** infosüsteemist või meedialt andmete kõrvaldamine nii, et neid ei ole võimalik tavavahenditega taastada.
- **AKREDITEERIMINE -** infosüsteemi turvalise funktsioneerimise formaalne kinnitus.
- **MISIOONIKRIITILISED SÜSTEEMID** – kõrgete turvanõuetega ja info suure väärtusega (turvaintsidendi korral suurte potentsiaalsete kahjudega) infosüsteemid.
- **KONFIDENTSIAALSUSLEPING** – leping, mille osapooled vastastikku kohustuvad mitte avaldama ühistöö käigus vastastikku avalikustatud konfidentsiaalset infot.
- **TURVAPERIMEETER** määratleb asutuse jaoks elutähtsa või tundliku informatsiooni töötlemiseks ja töötluse vahendite paiknemiseks turvalised alad, mis on volitamatu juurdepääsu, kahjustuste ja häiringute eest nii füüsiliselt kui ka infotehnoloogiliselt (FW, VPN, IDS, viirusetõrje jms) kaitstud.

  Eesmärk: vältida volitamata juurdepääsu tööruumidele ja informatsioonile, nende kahjustusi ja häiringuid.

- Infovara = info + infotöötlusressusrss
  Infotöötlusressusrss = infotöötlussüsteem + personal + infrastruktuur
  Infotöötlussüsteem = tarkvara + riistvara



- Infona käsitletakse andmeid elektronkujul (andmebaas, fail, meil), paberil, inimkõnes (vestlus, telefon, automaatvastaja, kõnepost) või muul kandjal, mida kasutatakse otsuste tegemisel, analüüsimisel jne.

- Infosüsteemipõhisemalt võib infovarasid defineerida ka järgmiselt:
    - andmed (elektronkujul)
    - IT-aparatuur (riistvara – serverid, kliendiarvutid, sideseadmed, toiteseadmed jm)
    - tarkvara – opsüsteemid, baastarkvara (*application enabling software* – andmebaasid, failiserverid, printserverid jms) ja rakendustarkvara
    - andmesidekanalid.

Selles juhendis käsitleme infovarana ja klassifitseerime digitaalkujul olevat infot, mis asub konkreetses infotöötlussüsteemis. Andmeturbenõuded püstitatakse üldjuhul kogu infosüsteemiga seotud andmetele(infole), erivajadusel ka üksikutele failidele, andmetabelitele, andmeväljadele või teatud päringutele ning sellega määratakse vastava infosüsteemi andmeturbe klass, mis omakorda määrab infosüsteemi andmeturbeks vajalike turvameetmete kompleksi.

4.1. ÜLDKOHALDUVAD TURVAMEETMED

(ei sõltu töödeldava informatsiooni turvaklassist)

TURVAORGANISATSIOON

1. Infoturbe poliitika/strateegia/organisatsioon
2. Infovarade kindlaksmääramine
3. Infovarade valdamine (valdamiskord, valdajate määramine), infovaradele turvanõuete määramine/infovarade klassifitseerimine
4. Infoturbe meetmete määratlemine (metoodika, kord)

VÕIMALIKUD ERINÕUDED INFOSÜSTEEMILE

5. Kuuluvus erikategooriasse
6. Nõuded tingitud seadustest, standarditest, eeskirjadest, lepingutest kolmandate osapooltega.

TURVAORGANISATSIOON

4.1.1. Infoturbe poliitika/strateegia/organisatsioon

1. Asutusel peab olema tippjuhtkonna poolt kinnitatud infoturbe poliitika ja strateegia ning loodud organisatsioon, kes vastutab infoturbe tegevuste, standardite ning protseduuride koostamise ja kehtestamise eest.
2. Vastav dokument tuleb kõigile ettevõtte töötajaile teha kättesaadavaks.
3. Infoturbe poliitika (lühivariandis) peaks olema esitatud:
    - põhiseisukoht info ja selle kaitsmise olulisuse kohta ettevõttele
    - juhi kohustus määrata asutuse infoturbe juht koos tema ülesannete loeteluga
    - asutuse personali kohustus jälgida infoturbeosakonna kehtestatud tegutsemisjuhiseid, standardeid ning protseduure asutuse töötajate kohustus jälgida ettevõttes kehtestatud korda, standardeid ning protseduure
4. Tuleb kehtestada reegel - "mis ei ole selgelt lubatav, on üldjuhul keelatud".

5. Vajalik ja nõutav on turbealase foorumi (näiteks Turvakomitee) loomine ja seda just juhtkonna teavitamiseks vastaval alal läbiviidavatest muudatustest.
6. Kõik toimunud turvaintsidendid tuleb ette kanda turvakomitees.
7. Komiteedes olevad inimesed ja nende kohustused tuleb perioodiliselt läbi vaadata ja kinnitada.

Ühispangas on selle läbiviimiseks olemas erinevad komiteed, kuhu kuuluvad samuti juhtkonna liikmed – turbe-, äri jne komiteed. Nende poolt toimub infoturbepoliitika heakskiitmine, turberollide määramine ja turbe evituse koordineerimine kogu organisatsiooni ulatuses.

8. Tuleb olla kursis turbe arengu ja muutustega, jälgida standardeid ja hindamismeetodeid.
9. Kõiki olemas olevaid infovarasid tuleb seirata tagamaks hilisem andmete kättesaadavus intsidendi puhul.

4.1.2. Infovarade kindlaksmääramine

1. Infovarade määratlemise eesmärk on tuvastada kõik turvatavad infovarad. Protsessi detailsel elluviimisel fikseeritakse juba rakendatud turvameetmed.
2. Infovarade nimistu on dokument, mis loetleb asutuse infovarad.
3. Iga infovara korral peab olema fikseeritud:
    - nimetus
    - valdaja
    - hetkeasukoht
    - infovara juba rakendatud turvameetmed
4. Infovarade nimistut tuleb hoida ajakohasena.

4.1.3. Infovarade valdamine

Valdajate määramine, valdamiskord, infovaradele turvanõuete määramine/infovarade klassifitseerimine

1. Juhtkond peab tagama, et kõigile infovaradele (infosüsteemidele) on määratud valdajad (owner).
2. Tuleb dokumenteerida valdajate turvarollid ja -kohustused sellisel kujul, nagu nad on sõnastatud organisatsiooni infoturbepoliitikas.
3. Rakenduse valdaja peab rakendussüsteemi infoturvanõuded selgekujuliselt määratlema ja dokumenteerima.
4. Olulisi äriprotsesse toetavate infosüsteemide valdamisdokumentatsioon peab samuti sisaldama teenuste, tarkvara, infovarade ja füüsiliste varade kirjeldusi.
5. Tuleb luua kord, millele vastavalt valdajad määratlevad ja hoiavad ajakohasena teatud kindlale salajasele infole juurdepääsuks volitatud gruppide nimistud.

4.1.4. Infoturbe meetmete määratlemine (metoodika, kord)

1. Peab olema valitud metoodika infoturbe meetmete valikuks.
2. Peab olema kehtestatud kord, millele vastavalt tegelikult toimub infoturbe meetmete valik.
3. Infoturbe metoodikat peab hoidma ajakohasena.

ERINÕUDED INFOTURBELE

Infosüsteemide infoturbe meetmete spetsifitseerimisel (nii esmakordsel kui ka perioodilisel testimisel/akrediteerimisel) tuleb kindlaks teha infosüsteemi võimalik kuuluvus mingisse erikategooriasse (st süsteemi võib adekvaatselt turvata ka ilma astmeliste turbemeetmeteta) ja/või lepingutest/seadustest jms tingitud spetsiifiliste erinõuete olemasolu ning sellest tulenevad vajalikud/lisanduvad turbemeetmed.

Tabel 1. Erinõuded infoturbele.

	Võimalikud erinõuded infosüsteemile
1	Kuuluvus erikategooriasse
2	Juriidilised nõuded : - nõuded lepingutest kolmandate osapooltega - nõuded tingitud seadustest, standarditest, eeskirjadest.

4.1.5. Erikategooriad

Mõningaid süsteeme võib adekvaatselt turvata ka ilma osas 4.3 kirjeldatud astmeliste turvameetmeteta. Sellised süsteemid ei ole "erandid" või "erijuhtumid", vaid sellistel juhtudel astmeliste turbemeetmete rakendamisega kaasneb liigne kulu.
Mitmete selliste spetsiaalsüsteemide (serverid, turvamoodulid, eriotstarbelised süsteemid) nõutav turvatase on saavutatav füüsiliste turbemeetmetega, kui süsteemide platvormi tarkvara tagab kasutajate ja nende poolt sooritatavate tehingute nõutava eraldatuse.
Spetsiaalsüsteeme iseloomustavad tunnused:

(a) süsteemis ei ole üldkasutajaid ega kasutajate programme,
(b) süsteemile omavad juurdepääsu ainult süsteemiadministraator ja hooldajad,
(c) süsteem osutab mitteinteraktiivset teenust (packet routing),
(d) üksikkasutuses olevad lokaalsed süsteemid.

1. Ettepaneku infosüsteemi kuuluvusest erikategooriasse teeb üldjuhul IT süsteemide hooldusjuht või andmeturbejuht ning kinnitab IT juht.
2. Infosüsteemi kuulumine mingisse erikategooriasse (spetsiaalsüsteemid, millistel vajalikud/kohustuslikud turvameetmed on kirjeldatud tehnilises dokumentatsioonis) välistavad vajaduse järgnevaks astmeliste turvameetmete määramiseks.

4.1.6. Vastavus juriidilistele nõuetele

1. Vajalike turvameetmete määratlemisel ja kohaldamisel tuleb lähtuda riiklikest seadustest ja standarditest ning asutuse sisemistest eeskirjadest.
2. Kolmandate osapoolte poolt tarnitavate teenuste ja infovarade turvameetmed ning samuti kolmanda osapoole juurdepääsu asutuste infosüsteemidele reguleeriv kord peab põhinema ametlikul lepingul, kus sisalduvad või kus viidatakse kõigile vajalikele turvatingimustele, mis ühtlasi peavad vastama ka asutuse turvapoliitikale ja standarditele.

4.2. *ASTMELISED TURVAMEETMED*

Määrame valdaja poolt turvatavale infole esitatud turvanõuetele vastavad vajalikud astmelised turvameetmed (Tabel 2. Astmeliste turvameetmete määratlemine):

- Määrame tabelis edasise töö aluseks olevad veerud vastavalt turvatava informatsiooni turvanõuetele/turvaklassifikaatoritele (vt Tabel 2 – hallid veerud).
- Leiame tabelis valitud (hallid) veergudest kõigile ridadele astme maksimumi reas (vt Tabel 2 – bold ja punane)- tulemus tabeli viimasesse veergu (vt Tabel 2 – bold/italic ja sinine **"**Vajalikud meetmete astmed - nõutavatele turvaklassifikaatoritele vastavalt meetme maksimaalne aste reas") – sisuliselt leidsime vajalikud meetmete astmed turvatavat infot töötleva infosüsteemi kõigile infotöötlusressurssidele.
- Vajalikele astmetele vastavate turvameetmete loetelud saame tabeli esimeses veerus toodud käesoleva juhendi sisukorrapunkti alt

ASTMELISTE TURVAMEETMETE JAOTUS/GRUPEERING
(sõltuvad töödeldava informatsiooni turvaklassist)**:**

TURVAORGANISATSIOON
1. Turvadokumentatsiooni/muudatuste haldus (DOK)
2. Infosüsteemide turvanõuetele vastavaks tunnistamine (TA)

PERSONAL
3. IT personalihaldus (ITP)
4. Töötajate instrueerimine, koolitus ja atesteerimine (IKA)

INFRASTRUKTUUR
5. Füüsiline turve
6. IS kasutajate tööruumid (TRM)
7. Spetsiaalruumid (serveri- ja sideruumid) (SRM)

INFOTEHNOLOOGILISED VAHENDID
8. Pääsuõigused (PÕ)
9. * Side (KOM)
10. * Välisperimeetri ja Välisühenduste Kaitse (VVK)
11. * Sisevõrgu Turve (SVT)
12. * Viiruste ja muu õelkoodi rünnete tuvastamine ning tõrje (VÕT)
13. Info krüpteerimine (KR)
14. Seire (MON)
15. IS kasutajate töö jälgimine (KJ)
16. Andmete varundamine ja taastamine (AVT)
17. IS hooldus (ISH)
18. Infoturvaintsidentide haldus (TIH)
19. IS arendus (ISA)
20. IS testimine (IST)
21. Ajakohastamine, kontroll ja turvatestimine (AKT)

TALITLUSPIDEVUS
22. Talitluspidevuse - ja taasteplaanid (TPT)
23. Infosüsteemide taasteplaanid (ISTP)

* Veel üks väga oluline põhimõte: küllalt tihti on mõttekas kasutada mingi kõrgete turvanõuetega missioonikriitilise infosüsteemi jaoks vajalikke ja juba juurutatud/juurutatavaid turvalahendusi ka vähemkriitiliste juures. Seda just seetõttu, et enamasti juba juurutatud turvalahendus(t)e kasutamine ka mujal ei põhjusta üldjuhul olulisi lisakulutusi. On muidugi võimalikud probleemis koormuse ja läbilaskevõimega, kuid nende lahendamiseks on kulutused ikka oluliselt väiksemad. Eriti kehtib see side-, välisperimeetri kaitse-, sisevõrgu turbe ja viiruste/õelkoodi kaitse lahenduste puhul – nendes valdkondades juba olemasolevate lahenduste mittekasutamine on mõttetu ja isegi lubamatu.

Tabel 2. Astmeliste turvameetmete määratlemine.

Meetmete loetelu/kirjelduse sisukorrapunkt	Informatsiooni infoturbe nõuded/klassifikaatorid / Infoturbeks vajalikud ressursid/tegevused. Sisuliselt oluliste infoturbe tegevusvaldkondade loetelu. Need omakorda sisaldavad juba vajalikke konkreetseid turvameetmed.	Konfidentsiaalsuse nõue/klassifikaator				Käideldavuse nõuded/klassifikaatorid								Tervikluse nõue/klassifikaator				Vajalikud meetmete astmed - nõutavatele turvaklassifikaatoritele vastavalt meetme maksimaalne aste reas
						Aegkriitilisus				Hilinemise tagajärgede kaalukus								
		S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3	
		Avalikud andmed	Andmed sisemiseks kasutamiseks	Salajased andmed	Eriti salajased andmed	Andmete hilinemine ei põhjusta probleeme	Lubatav andmete mõnepäevane hilinemine	Andmed tuleb saada mõne tunni jooksul	Andmed tuleb saada sekundite jooksul	Andmete õigeaegne mittesaamine ei põhjusta olulisi tagajärgi	mittesaamine võib põhjustada takistusi Infosüsteemi funktsiooni (ja vastava põhitegevusfunktsiooni)	saamine toob kaasa olulisi takistusi Infosüsteemi funktsiooni (ja vastava põhitegevusfunktsiooni)	mittesaamine toob kaasa Infosüsteemi funktsiooni (ja vastava põhitegevusfunktsiooni)	Muutmiste kaitse/tuvastamine pole vajalik	Volitamata muutmiste kaitse/tuvastamine	Sisestaja/muutja peab olema tõestatav (n kohtus)	Sisestaja/muutja peab olema tõestatav (n kohtus)	
	TURVAORGANISATSIOON																	
4.2.1	**Turvadokumentatsioon**	DOK-1	DOK-2	DOK-3	DOK-4	DOK-1	DOK-2	**DOK-3**	DOK-4					DOK-1	DOK-2	DOK-3	DOK-4	***DOK-3***
4.2.2	**IS turbe akrediteerimine**		TA-1	TA-1	TA-2		TA-1	**TA-1**	TA-2						TA-1	TA-1	TA-2	***TA-2***
	PERSONAL																	
4.2.3	**IT Personalihaldus**		ITP-1	ITP-2	ITP-2		ITP-1	ITP-2	ITP-2				**ITP-3**		ITP-1	ITP-2	ITP-2	***ITP-3***
4.2.4	**Töötajate instrueerimine ja koolitus**		IKA-1	IKA-2	IKA-3		IKA-1	**IKA-2**	IKA-3						IKA-1	IKA-2	IKA-3	***IKA-2***
	INFRASTRUKTUUR																	
4.2.5	**Füüsiline turve**	FT-1	FT-2	FT-3	FT-4	FT-1	FT-2	**FT-3**	FT-3					FT-1	FT-2	FT-3	FT-4	***FT-3***
4.2.6	**IS lõppkasutajate tööruumid**	TRM-1	**TRM-1**	TRM-2	TRM-2				TRM-3						**TRM-1**	TRM-2	TRM-3	***TRM-2***
4.2.7	**Serveriruumid**		SRM-1	SRM-2	SRM-3		SRM-1	SRM-2	SRM-3				**SRM-4**		SRM-1	SRM-2	SRM-3	***SRM-4***
	INFOTEHNOLOOGILISED VAHENDID																	
4.2.8	**Pääsuõiguste haldus**	PÕ-1	PÕ-2	PÕ-3	PÕ-4	PÕ-1	PÕ-2	**PÕ-3**	PÕ-3					PÕ-1	PÕ-2	PÕ-3	PÕ-4	***PÕ-3***
4.2.9	**Side**	KOM-1	KOM-1	KOM-2	KOM-3	KOM-1	KOM-1	KOM-2	KOM-2				**KOM-4**	KOM-1	KOM-1	KOM-2	KOM-3	***KOM-4***
4.2.10	**Välisühenduste ja välisperimeetri kaitse**		VVK-1	VVK-2	VVK-3		VVK-1	**VVK-2**	VVK-3						VVK-1	VVK-2	VVK-3	***VVK-2***
4.2.11	**Sisevõrgu Turve**	SVT-1	SVT-1	SVT-2	SVT-3	SVT-1	SVT-1	**SVT-2**	SVT-3					SVT-1	SVT-1	SVT-2	SVT-3	***SVT-2***
4.2.12	**Viiruste ja õelkoodi tuvastamine ning tõrje**	VÕT-1	VÕT-1	VÕT-2	VÕT-3	VÕT-1	VÕT-1	**VÕT-2**	VÕT-3					VÕT-1	VÕT-1	VÕT-2	VÕT-3	***VÕT-2***
4.2.13	**Info krüpteerimine**																	
	Krüpteerimine		**KR-K1**	KR-K2	KR-K3													***KR-K1***
	Pääsukontroll		KR-P1	KR-P2	KR-P3		KR-P1	**KR-P2**	KR-P3						KR-P1	KR-P2	KR-P3	***KR-P2***
	Tervikluskontroll													KR-T1	KR-T2	KR-T3	KR-T4	
	Võtmehaldus	KR-V1	**KR-V2**	KR-V3	KR-V4			**KR-V2**	KR-V3					KR-V1	**KR-V2**	KR-V3	KR-V4	***KR-V2***
4.2.14	**Seire**	MON-1	MON-2	MON-3	MON-4	MON-1	MON-2	**MON-3**	MON-4					MON-1	MON-2	MON-3	MON-4	***MON-3***
4.2.15	**IS kasutajate töö jälgimine**	KJ-1	KJ-2	KJ-3	KJ-4	KJ-1	KJ-2	**KJ-3**	KJ-4					KJ-1	KJ-2	KJ-3	KJ-4	***KJ-3***
4.2.16	**Andmete varundamine ja taastamine**		AVT-1	AVT-2	AVT-3		AVT-1	**AVT-2**	AVT-3						AVT-1	AVT-2	AVT-3	***AVT-2***
4.2.17	**IS hooldus**		ISH-1	ISH-2	ISH-2		ISH-1	**ISH-2**	ISH-2						ISH-1	ISH-2	ISH-2	***ISH-2***
4.2.18	**Infoturvaintsidentide haldus**		TIH-1	TIH-2	TIH-2		TIH-1	**TIH-2**	TIH-2						TIH-1	TIH-2	TIH-2	***TIH-2***
4.2.19	**IS arendus**		ISA-1	ISA-2	ISA-2		ISA-1	**ISA-2**	ISA-2						ISA-1	ISA-2	ISA-2	***ISA-2***
4.2.20	**IS testimine**		IST-1	IST-2	IST-2		IST-1	**IST-2**	IST-2						IST-1	IST-2	IST-2	***IST-2***
4.2.21	**Ajakohastamine, kontroll ja turvatestimine**		**AKT-1**	AKT-2	AKT-3				AKT-1						**AKT-1**	AKT-2	AKT-3	***AKT-1***
	TALITLUSPIDEVUS																	
4.2.22	**Talitluspidevus ja taaste**						TPT-1	TPT-2	TPT-3		TPT-1	TPT-2	**TPT-3**					***TPT-3***
4.2.23	**Infosüsteemide taaste**		ISTP-1	ISTP-2	ISTP-3		ISTP-1	ISTP-2	ISTP-3		ISTP-1	ISTP-2	**ISTP-3**		ISTP-1	ISTP-2	ISTP-3	***ISTP-3***

4.2.1. Turvadokumentatsioon (DOK)

Turvadokumentatsioon on süsteemide turbe alusdokument ja ühtlasi tõendus selle kohta, et süsteem või olemasoleva süsteemi muudatus vastab süsteemile esitatavatele turvanõuetele. Turvadokumentatsiooni kasutatakse kogu süsteemi elutsükli jooksul, kui dokumenti, mis kirjeldab süsteemi ja selle käitluskeskkonda. Turbe konfiguratsiooni ja muudatuste haldusega tagatakse, et ajakohased turvameetmed on süsteemis juurutatud ja nende ülalhoid korraldatud. Turvadokumentatsioon on ka süsteemi inspekteerimise aluseks.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Turvadokumentatsioon ja muudatuste haldus	DOK-1	DOK-2	DOK-3	DOK-4	DOK-1	DOK-2	DOK-3	DOK-4					DOK-1	DOK-2	DOK-3	DOK-4

DOK-1

Tegemist on süsteemiga millegi proovimiseks/enesearenduseks ja süsteemis sisalduva informatsiooni turvaklass (**edaspidi süsteemi turvaklass)** on S0K0R0T0**.**

Turvadokumentatsioon peab sisaldama:

1. Süsteemi identifikaatorit;
2. Süsteemi valdaja nime;
3. Mõnerealist kirjeldus süsteemi otstarbest ja võrgukasutusest;
4. Süsteemis sisalduva informatsiooni turvaklassi (Peab olema fikseeritud, et süsteemis sisalduva informatsiooni turvaklass on S0K0R0T0).

DOK-2

Kuna infosüsteem pole kriitiline, siis on üldjuhul aega otsida konkreetset administraatorit, kes probleemi lahendaks – vajalik valdaja ja IT administraatori(te) kontaktinfo, infosüsteemi riistvara ja tarkvara lühikirjeldus

Turvadokumentatsioon peab sisaldama:

5. Süsteemi valdaja, serveri- ja rakenduse administraatori(te) nime(sid), telefoninumbrit(reid) ning serveri tähistust ja asukohta.
6. Lühi kirjeldust süsteemi otstarbest ja võrgukasutusest (alamvõrgud, kommunikatsiooniseadmed ja –protokollid, süsteemikomponentide omavahelised seosed ja välised ühendused teiste süsteemidega jms).
7. Süsteemi kõikide unikaalsete riskide ja nõrkuste ja vastavate turvameetmete kirjeldust. Kui ei eksisteeri süsteemi suhtes unikaalseid ohtusid või nõrkusi tuleb see ka kirjelduses fikseerida.
8. Süsteemi turvaklassi ning turvameetmete loetelu.
9. Lühikest kirjeldust, kuidas süsteemis on juurutatud turvameetmed.
10. Turvanõuete tagamise kinnitus: andmeturbejuhi (IT juhi) kinnitus selle kohta, et kõik turvanõuete täitmiseks vajalikud turvameetmed on kohaldatud.
11. Turbe konfiguratsiooni ja -muudatuste juhtimise dokumentatsioon: peavad olemas olema protseduurid muudatuste (rakendused, rakenduste platvormid, ühenduste riist- ja tarkvara) dokumenteerimiseks. Muudatuste juhtimine peab käsitlema

infosüsteemi(de) kõiki modifikatsioone.

12. Üldiseid turvanõuded infosüsteemide hoolduse korraldamisele ja konkreetseid lisanõudeid hooldusele, sõltuvalt töid teostavast personalist (asutusesisene või kaughooldus; asutusesisene või asutuseväline hoolduspersonal jms).
13. Koopiad IS serverite konfiguratsioonidest elektroonselt (soovitavalt ka paberil) ning soovitavalt ka kasutajate arvutite konfiguratsioonidest.
14. Konfidentsiaalset informatsiooni käsitlevas dokumendis peab olema selgesõnaliselt ja arusaadavalt kõikidel lehtedel kirjutatud raporti salajasuse aste (sisemiseks kasutuseks, salajane, ülisalajane), nii et see tagab märgendite viivitamatu mõistmise ja informatsiooni asjakohase kaitse. Vastavasisuline märgend peab olema kättesaadav vaid selleks volitatud inimestele.

DOK-3

Kriitiline infosüsteem ja dokumentatsioon peab olema sellisel tasemel, et taastada suudab ka dubleeriv administraator, st on oluline, et süsteemi kirjeldus oleks selleks piisavalt üksikasjalik ja ajakohane.

Turvadokumentatsioon peab sisaldama:

15. Turvadokumentatsioon peab sisaldama piisavalt põhjalikku kirjeldust süsteemi otstarbest, arhitektuurist ja võrgukasutusest (alamvõrgud, sideseadmed, kommunikatsiooniprotokollid, blokkdiagramm, mis näitab süsteemikomponentide omavahelisi ja väliseid ühendusi teiste süsteemidega jms).
16. Muudatustega seotud turvakontroll: kõik andmeturbega seotud modifikatsioonid (s.h. tarkvara, riistvara või liidesed või võrguühendused) peavad olema kontrollitud ja see ka kirjalikult fikseeritud (vastavalt muudatuse jõustamise korrale).
17. Peab olema raport sõltumatult (sõltumatu grupp võib olla nii maja sisene (näiteks audit) kui väline) infoturbe testimise grupilt dokumentatsiooni ajakohasuse kohta oluliste muudatuste korral või vähemalt kord viie aasta jooksul.
18. Dokumenteeritud ja rakendatud peavad olema andmeturbe kontrollprotseduurid: nii muudatuste kui ka ekspluatatsiooni jaoks kes, mida, perioodilisus jms.
19. Kirjeldusi olulistest ja spetsiifilistest süsteemi installeerimis-, administreerimis- jms tööoperatsioonidest.

DOK-4

20. Dokumentatsioon sellisel tasemel, et taastada suudab ka suvaline valdkonda tundev spetsialist - st oluline, et muudatustele lisaks dokumenteeritud ja ajakohased ka installatsioonijuhendid, koopiad konfiguratsioonifailidest, andmete kirjeldused jms.

4.2.2. Infosüsteemide turvanõuetele vastavaks tunnistamine (TA)

(Infosüsteemi turbe akrediteerimine)

Turbe akrediteerimise eesmärk on kinnitada süsteemi turvameetmete korrektne toimimine ning kinnitada, et ettenähtud turvameetmed on kooskõlas *lõplike* turvenõuetega, on evitatud ja toimivad korrektselt. Akrediteerimisprotsess algab peale

turvameetmete evitamist ja kui kogu vajalik infosüsteemide dokumentatsioon on kinnitatud.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS turbe akrediteerimine		TA-1	TA-1	TA-2		TA-1	TA-1	TA-2						TA-1	TA-1	TA-2

TA-1 (hindamine)

1. Juurdepääs informatsioonile peab vastama seadustele, reeglitele ja eeskirjadele selles jurisdiktsioonis, kus asub süsteem (Eesti Riik ja SEB grupp)
2. Kõik auditipoolsed tegevused ja pöördused süsteemi poole tuleb seirata ja logida kontrolljälje loomiseks
3. Infosüsteemide riist- ja tarkvara sobivust tuleb hinnata enne kasutamist (üldtunnustatus, asutuse IT spetsialistide kogemused jms).
4. Struktuuriüksustes paiknevate infosüsteemide turvadokumentatsiooni ja infosüsteemi akrediteerimist koordineerib andmeturbejuht. Ülevaateraport tuleb saata siseauditile.
5. Andmeturbejuht peab üle vaatama ja akrediteerima kõik süsteemid enne nende töösse rakendamist neis töödeldatava informatsiooni konfidentsiaalsuse, käideldavuse ja tervikluse ning töötlemiseks vajaliku jõudluse tagamiseks.
6. Andmeturbejuht võib lubada ajutise akrediteeringu süsteemi puuduliku dokumentatsiooni tõttu või suure infosüsteemi muudatuse läbiviimiseks. Ajutise akrediteeringu kestus võib olla kuni 180 päeva. Ajutise akrediteerimise perioodil peavad olema rakendatud andmeturbejuhi poolt määratud turbemeetmed.
7. Akrediteering muutub kehtetuks koheselt kui toimuvad süsteemide turvet mõjutavad muudatused selle toimimiskeskkonnas või liidestes/ühendustes.
8. Perioodiline hindamine: kord viie aasta jooksul peab andmeturbejuhi koordineerimisel läbi viima juurutatud süsteemide turvalisuse hindamise (oluliste intsidentide puudumisel ja intsidentide korral vastavalt vajadusele).
9. Akrediteerimine erijuhtudel (turvaintsident, oluline muutus jms): kontrollitakse (audit või andmeturbejuht), et turvafunktsioonid ei oma soovimatuid kõrvalmõjusid, tulemused dokumenteeritakse ja andmeturbejuht peab otsustama võimalike ja vajalike muudatuste ning paranduslike tegevuste üle.
10. Juhul kui süsteemile kohaldatud turbemeetmed ei osutu piisavaks või toimuvad muutused tehnilistes või mittetehnilistes turbemeetmetes, infosüsteemi nõrkustes, toimimiskeskkonnas või toimimiskontseptsioonis, peab andmeturbejuht akrediteerimise tühistama ja algatama uute lahenduste väljatöötamise.

TA-2 (testimine, sõltumatu kontroll)**.**

11. Sõltumatu infoturbegrupp peab turvajuhi koordineerimisel olema nõuandjaks infosüsteemide akrediteerimistestide vajaduste väljaselgitamisel
12. Sõltumatu kontroll: toimunud turvaintsidentide või ilmnenud uute potentsiaalsete turvariskide puhul peab läbi viima akrediteerimisteste, kaasates võimaluse ja vajaduse korral testide läbiviimisel ka sõltumatuid infoturbeeksperte ja -gruppe.

    Sõltumatu kontrolli käigus tuleb saada erapooletu kinnitus teemadel (vastavalt vajadusele ja püstitatud eesmärgile ühele või enamale):

- IT-teenuste toimivuse sõltumatu hindamine
- Väliste teenuste tarnijate teenuste lubatud (kokkulepitud) kvaliteedi ja toimivuse sõltumatu hindamine.
- Seaduste ja eeskirjade nõuetele ning lepingukohustustele vastavuse tagatus
- Seaduste ja eeskirjade nõuetele ning lepingukohustustele vastavuse tagatus väliste teenuseandjate puhul

PERSONAL

4.2.3. IT personali haldus (ITP)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IT personalihaldus		ITP-1	ITP-2	ITP-2		ITP-1	ITP-2	ITP-2				ITP-3		ITP-1	ITP-2	ITP-2

ITP-1

1. Tuleb hinnata suuremate muudatuste korral põhitegevus-, ekspluatatsiooni- või infotehnoloogiakeskkonnas personali vajaduse ja kvalifikatsiooni nõudeid. Hindamistulemuste alusel tuleb asjakohaselt tegutseda, nii et oleks tagatud adekvaatne personali hulk ja vastutuse jaotus.
2. Personali värbamisel ja valikul tuleb eelnevalt teha taustuuring (kriminaalregister, krediidiinfo, teave endistelt tööandjatelt), intervjuu ning vajadusel narkotest.
3. IT juhtkond peab tagama, et kõigil IT töötajail oleksid infosüsteemide suhtes oma rollid ja vastutused ja et nad teaksid neid. Kogu personalil peavad olema piisavad volitused talle määratud rollide ja vastutuste täitmiseks. Igaüks peab olema teadlik sellest, et tal on teatav vastutus sisejuhtimise ja turvalisuse eest. Seetõttu tuleb teadlikkuse ja distsipliini tõstmiseks organiseerida ja läbi viia regulaarseid kampaaniaid.
4. IT juht peab tagama, et kehtestatakse IT personali ametijuhendid ja et neid värskendataks regulaarselt. Need ametijuhendid peavad selgelt sõnastama õigused ja kohustused, sisaldama vastava ametikoha jaoks nõutavate oskuste ja kogemuste määratlusi ning sobima kasutamiseks töönäitajate hindamisel.
5. Infosüsteemide omandus ja valdamine: juhtkond peab looma teatava struktuuri andmete omanike ja valdajate ametlikuks määramiseks. Nende rollid ja vastutused peavad olema selgelt määratletud. Juhtkond peab tagama, et kõigile infovaradele (infosüsteemidele) on määratud valdajad, kes teevad otsuseid info turvanõuete ja pääsuõiguste kohta. Tavaliselt delegeerivad info (esma)valdajad infosüsteemi(de) hoolduse IT ekspluatatsioonirühmale, turvakohustused aga andmeturbejuhile. Asjakohaste turvameetmete käigushoiu eest jäävad aga infovarade omaniku ees esmavastutavaiks esmavaldajad. (Peadirektori käskkiri, et andmete valdajaks on põhitegevusvaldkond ja infotöötlusvahendite valdajaks IT osakond.)
6. IT juhtkond peab IT töötajaile ametijuhendis määratlema vastutuse kvaliteedi tagamise funktsiooni täitmise eest ja tagama, et infoteenuste kvaliteedi tagamisega tegeleval IT personalil oleks vajalik asjatundmine kvaliteedi tagamise, süsteemide, juhtimismeetmete ja side alal.
7. Asutuse juht peab ametlikult määrama vastutuse organisatsiooni infovarade loogilise ja füüsilise turbe tagamise eest andmeturbejuhile, kes annab aru asutuse juhile.

Turbehalduse alane vastutus organisatsiooni üldiste turvaküsimustega tegelemiseks tuleb kehtestada vähemalt üleorganisatsioonilisel tasemel.

8. IT juhtkond peab infoteenuste organisatsioonis evitama adekvaatsed järelevalveviisid, mis tagavad, et rolle ja kohustusi täidetakse korralikult, et saaks otsustada, kas kõigil töötajail on oma rollide ja kohustuste täitmiseks piisavalt võimu ja ressursse.
9. Juhtkond peab määratlema ja evitama asjakohased protseduurid infoteenuste funktsiooni konsultantide ja muu lepingulise personali tegevuste juhtimiseks, et tagada organisatsiooni infovarade kaitse – lepingutes ka andmeturbe punktid, konfidentsiaalsuslepe jms
10. IT juhtkond peab rakendama vajalikke meetmeid optimaalse koordinatsiooni-, teavitus- ja sidestruktuuri rajamiseks ja käigushoiuks IT ja mitmesuguste teiste huvipoolte vahel (kasutajad, koostööpartnerid).
11. Töölepingusse tuleb lülitada töötaja õigusalased kohustused ja õigused (näiteks autoriõiguseseaduste või andmekaitseseaduste mõttes).

Inimressursside haldus:

12. Personalihaldus peab evitama ja regulaarselt hindama vajalikud protsessid, mis tagavad, et personali värbamise ja edutamise tavad põhineksid objektiivsetel kriteeriumidel ning arvestaksid haridust, kogemust ja vastutust. Need protsessid peavad olema kooskõlas organisatsiooni üldiste poliitikate ja protseduuride vastava osaga.
13. IT juhtkond peab regulaarselt kontrollima (n arenguvestlused), kas teatavaid ülesandeid täitev personal vastab oma kvalifikatsioonilt sellekohastele haridus-, koolitus- ja/või kogemusnõuetele.
14. Personalihaldus peab evitama töötajate hindamise (arenguvestluste) ja atesteerimise protsessi ning tagama, et hindamine toimuks regulaarselt ning võrdlemise teel kehtivate standarditega ja konkreetsete töökohustustega.
15. Personalihaldus ja IT juhtkond peab tagama, et IT töötajaid nende palkamisel instrueeritakse ning et pideva koolitusega hoitakse nende teadmised, oskused, võimed ja turvateadlikkus vajalikul tasemel. Personali tehniliste ja haldusoskuste taseme tõstmiseks läbiviidavaid haridus- ja koolitusprogrammid peavad toimuma regulaarselt ja temaatikat tuleb regulaarselt ajakohastada.
16. IT juhtkond peab tagama, et IT personal enne töölevõttu, ümberpaigutamist või edutamist läbib turvakontrolli, mis sõltub vastava ametikoha missioonikriitilisusest ja info konfidentsiaalsusest. Töötajat, kes sellist kontrolli ei ole läbinud, ei tohi paigutada missioonikriitilisele ametikohale.
17. *Personali ümberpaigutamine*: Personalihaldus ja IT juhtkond peavad tagama asjakohaste ja õigeaegsete meetmete rakendamise infovarade valdajate teisele töökohale üleviimiste puhul, sellised juhtumid ei tohi kahjustada sisejuhtimist ega turvalisust.
18. *Töösuhte lõpetamine*: informeerida Füüsilise - ja Andmeturbe osakondi, lahkumisintervjuu, omandi kontroll ja loovutamine, õiguste äravõtmine, tööruumide külastamise keeld, võtme(te) tagastamine, kasutajanime(de)/parooli(de) peatamine) (teostatus fikseeritakse ringkäigu lehel).

ITP-2

19. Peab kindlustama teatud funktsioonide lahususe, mis välistab võimaluse, et mingi üksikisik saaks oluliselt nõrgestada mingit kriitilist protsessi. Juhtkond peab hoolitsema ka selle eest, et töötajad täidaksid ainult neid ülesandeid, mis on neile pandud ametijuhendite ja ametikohtadega. Eriti tuleb hoida lahus järgmiste funktsioonide kohustused:
    - infosüsteemi administreerimine ja selle poolt teostatava/toetatava põhitegevusfunktsiooni kasutaja (kasutajad ei saa ligi adminstreerimisinfole ja vastupidi);
    - põhitegevusinfoüsteemide ja tugisüsteemide haldus;
    - infosüsteemide arendus ja hooldus;
    - turvahaldus ja turvaaudit.
20. Missioonikriitiliste infosüsteemide haldus- ja turvapersonal peab olema dubleeritud – peab olema tagatud, et neil töötajail oleksid asendajad ja/või antakse piisavalt ristkoolitust.

ITP-3

21. Missioonikriitiliste (kõrged turvanõuded, suured potentsiaalsed kahjud) 7x24 süsteemide personalitarve: tuleb arvestada vähemalt 2-kordse personalivajadusega (võrreldes analoogsete mittemissioonikriitiliste infosüsteemidaga ning personaliga tagatust tuleb hinnata vähemalt kord aastas või suuremate muudatuste korral põhitegevus-, ekspluatatsiooni- või infotehnoloogiakeskkonnas.

4.2.4. IT personali ja IS kasutajate instrueerimine, koolitus ja atesteerimine (IKA)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Töötajate instrueerimine ja koolitus		IKA-1	IKA-2	IKA-3		IKA-1	IKA-2	IKA-3						IKA-1	IKA-2	IKA-3

IKA-1

Instrueerimine - töötajale tuleb anda vastavad kirjalikud materjalid ja võtta allkiri kohustusele neid järgida.

1. Uutele töötajatele tuleb selgitada IT-ga seotud sisemisi eeskirju, tööpraktikaid ja protseduure (õigused ja kohustused seoses ametiga, turvaabinõude praktika töökohas, võtmed, paroolid). Näiteks:
    - kohustama kasutajad nende ajutisi paroole vahetama koheselt esimesel sisselogimisel;
    - tuleb kasutada turvalisi paroole, paroole ei tohi märkida paberile, kui seda üleskirjutust ei saa säilitada turvaliselt.
2. Töötajatele tuleb tutvustada turvaeeskirju ning kohustada ja motiveerida neid järgima (konfidentsiaalsuslepingu ja ametikohustuste allkirjastamine).
3. Tuleb abistada/nõustada infosüsteemide kasutajaid.
4. Mobiilseid töövahendeid kasutavat personali tuleb täiendavalt instrueerida teadvustamaks lisariskidest ja rakendatavatest lisaturvameetmetest.
5. Tuleb kehtestada ja tutvustada kasutajatele instruktsioone grupitöö vahendite kasutamise kohta.

IKA-2

Lisandub koolitus - rakenduste väära kasutamise vältimiseks tuleb kasutajad eelnevalt koolitada.

6. Tuleb välja selgitada süsteemiga töötava personali koolitusvajadused antud süsteemiga töötamiseks ja vastavad koolitus(ed) organiseerida. Enne süsteemi uutele kasutajatele kasutusõiguste andmist, tuleb nad eelnevalt koolitada.
7. Turvaprintsiipide ja -teadlikkuse koolitus: olulisemate ja keerukamate infoturbe valdkondadega kokku puutuv/seotud personal peab läbima vastava(d) spetsiaalse(d) koolitusprogrammi(d).
8. Abiliin ettevõtte töötajatele: põhitööajal peab olema tagatud infosüsteemide kasutajate pidev abistamine/nõustamine.

IKA-3

Lisandub atesteerimine – missioonikriitiliste rakenduste puhul peab olema tagatud kasutajate teadmiste ja oskuste nõutav tase.

9. Vajalik töötajate atesteerimine tööleasumisel ning edaspidi perioodiliselt, vajadusel täiendav koolitus.

INFRASTRUKTUUR

4.2.5. Füüsiline turve (FT)

Turvalisus on alati kahesuunaline – st asutuses peab nii töötaja kui ka klient/külastaja tundma ennast turvaliselt ja kaitstult väliste rünnete suhtes.

Füüsilise turvalisuse all mõistetakse:

- häiresüsteemide olemasolu
- uste, lukkude, seifide ja dokumendikappide olemasolu
- väärtuste transportimist
- töökohtade turvalisuse tagamise tehnikat
- andmete ja dokumentide säilitamise, hävitamise, transportimise ja hoidmise kaitset

Füüsilise turvalisuse tagamisega seotud infosüsteemid vajavad andmeturvet samuti nagu suvaline (põhitegevus)infosüsteem.

TURVALISUS TAGATAKSE JÄRGMISTE TEHNILISTE VAHENDITE SÜSTEEMIDEGA NING ORGANISATSIOONILISTE ABINÕUDEGA:

- videovalve
- kontroll-läbipääsu süsteem
- valvesignalisatsioon
- paanika signalisatsioon
- tulekahjuhäiresüsteemid
- tehniline valve
- julgestus teenus
- lukustus
- sertifitseeritud varahoidlad
- sertifitseeritud modulaarsed tulekindlad hoidlad infokandjate arhiveerimiseks ja hoidmiseks
- sertifitseeritud seifid, dokumendikapid, infokandjate kapid

- hoonete ja väärtuste kindlustamine
- juhendid, eeskirjad, korraldused ja käskkirjad
- turvaalane koolitus

IT Füüsiline turve:

- hoone turvalisus ja kaitse, sh teenuste kaitse
- volitamata hõive välistamine
- arvutitele juurdepääsu kontroll
- andmekandjatele juurdepääsu kontroll
- personali kaitse
- piksekaitse, kahjutule ja vee kaitse
- ohtude avastamine ja teatamine
- seadmete kaitse varguse eest
- ruumide teeninduse ja hoolduse reguleerimine

Personali isikukaitse:

- Piiritletakse isikukaitset vajavate töötajate ring
- Tehakse vastavad täiendused selliste töötajate töölepingusse
- Kaardistatakse isikukaitset vajavate töötajate töö ja kodused aadressid, telefoni ja auto numbrid, liikumise põhimarsruudid, perekonnaliikmete andmed jm., mis on vajalik teada isikukaitse tagamiseks.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Füüsiline turve	FT-1	FT-2	FT-3	FT-4	FT-1	FT-2	FT-3	FT-3					FT-1	FT-2	FT-3	FT-4

FT- 1

Üldkasutatavad tööruumid, kuhu juurdepääs võimalik ka klientidel/külastajatel.

1. Hoone ja olulised ruumid selles peavad olema pääsuteenistuse valve all
2. Peavad olema evitatud meetmed hoone, selles paikneva infotehnika (arvutid, sideseadmed, andmekandjad, vajalikud lisaseadmed – konditsioneerid, UPS'id jms) ja personali kaitseks.
3. Infotehnoloogia üld-infrastruktuurile peab kooskõlas üldise turvapoliitikaga olema kehtestatud asjakohased pääsu reguleerimise meetmed, kaasa arvatud infovahendite kasutamine väljapool organisatsiooni territooriumi. Pääs tuleb piirata, andes selle vaid isikuile, kellel on volitus niisuguseks pääsuks.
4. Konfidentsiaalset infot ja ettevõttele kuuluvaid seadmeid ei tohi omavoliliselt kõrvaldada. Juhul, kui selleks on tungiv vajadus, peab juhtkonnalt saama vastavasisulise volituse.
5. Kõik ettevõtte ruumidest välja viidavad ettevõtte seadmed tuleb registreerida.
6. Tuleb evitada tervishoiu ja tööohutuse alased toimimistavad, hoides neid kooskõlas asjakohaste rahvusvaheliste ja kohalike seaduste ning eeskirjadega.
7. Asutus(t)e hoone(te) haldusega tegelev inimene peab tagama piisavate meetmete evitamise ja korrigeerimise kaitseks keskkonnategurite (nt tuli, tolm, energiavarustus, ülemäärane kuumus ja niiskus) eest. Keskkonna seireks ja reguleerimiseks tuleb paigaldada eriseadmed.
8. Infosüsteemide ja side seisukohalt olulised ruumid peab IT juhtkond võtma oma täiendava (IT spetsiifilise) kontrolli ja jälgimise alla.
9. Tuleb tagada väljaspool ettevõtet olevate seadmete kindlustatus ning kinnitama need

lepingutega (näiteks turvafirmade kaudu ATM jne).

FT- 2 .

Ametiruumid/töökohad - asutuse sisemised tööruumid, kuhu võõraste juurdepääs lubatud ainult koos saatjaga

10. Kogu personalilt tuleb nõuda mingi nähtava identifikaatori kandmist ning töötajaid tuleb õhutada kontrollima saatjata võõraid ning kõiki, kes ei kanna nähtavat identifikaatorit.
11. Peab olema välistatud külastajate saatjateta juurdepääs, peavad kehtima protseduurid, mis tagavad, et kui külastajad peavad sisenema tööruumidesse, kus paiknevad infosüsteemi(de) lõppkasutajate arvutitöökohad, saadab neid asutuse töötaja.
12. Ruumid peavad üldjuhul olema lukustatud (kui oma personali sees pole, siis kindlasti lukus).
13. Tuleb pidada külastajate asutuse ruumidesse/asutuse turvaperimeetrisse sisenemiste päevikut.

FT- 3.

Tehnilised - ja salajase info töötlemisega seotud ruumid:

14. Ruumi pääseb ainult selleks volitatud personal vastavalt nimekirjale, mille kinnitab asutuse juht. Peavad kehtima protseduurid, mis tagavad, et kui ruumi peavad sisenema isikud, kes ei oma selleks luba, saadab neid volitust omav isik.
15. Ilma eriloata ei tohi tuua ettevõtte salajase ja ülisalajase info töötlemisega seotud ruumidesse foto-, video-, heli- või muud salvestusaparatuuri;

FT- 4.

Kriitilised tehnilised – ja ülisalajase info töötlemisega seotud ruumid:

16. Tuleb pidada külastajate päevikut ja seda regulaarselt läbi vaadata.
17. Dokumentide kontrollimine: loetava info osas tuleb läbi viia vaatlus, et enne asutuse infosüsteemi turvaperimeetri piiridest väljastamist oleks see korrektselt märgendatud ning sisaldaks asjakohast turvamarkeeringut (üldjuhul tähendab see, et valvelauas tuleb inimesi kontrollida põhjendatud kahtluse korral või näiteks ka pisteliselt, lauskontroll on praktiliselt väga raskelt realiseeritav).
18. Elektroonsel kujul oleva ainult sisemiseks kasutamiseks ja salajase/ülisalajase info turvaperimeetri piiridest väljaviimine on üldjuhul keelatud. Erijuhtudeks peavad olema kinnitatud spetsiaalsed korrad võimalikult piiratud inimeste nimistule või vajalik ettevõtte tippjuhtkonna eriluba.

4.2.6. IS lõppkasutajate tööruumid (TRM)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS lõppkasutajate tööruumid	TRM-1	TRM-1	TRM-2	TRM-3				TRM-3						TRM-1	TRM-2	TRM-3

TRM-1 (asutuse sisemised tööruumid)**.**

1. Ruumid peavad vastama kehtivatele IT spetsiifilistele turvaeeskirjadele ja standarditele.
2. Tuleb määratleda ruumid/alad, kus on lubatud süüa, juua ja suitsetada.
3. Protseduuriliselt peab olema kindlustatud, et kõik infosüsteemi riistvara komponendid sh. sisend/väljundseadmed, omavad nähtavat märgistust (inventarinumbrit).

TRM-2
(asutuse sisesed tööruumid, kus tegemist delikaatse isikuinfoga jm salajase infoga).

4. Perioodiliselt tuleb läbi viia tehnovõrkude vajadustele vastavuse kontrolli ning vajadusel kaasajastada dokumentatsioon.
5. Puuduste/probleemide ilmnemisel peab toimuma kohene tehnovõrkude täiustamine/kontroll ning vastava dokumentatsiooni kaasajastamine.
6. Seadmed, mis kuvavad või väljastavad informatsiooni loetavas vormis, peavad olema paigutatud selliselt, et volitamata isikud ei saaks neilt lugeda informatsiooni ilma süsteemikasutaja loata/teadmiseta, vajadusel tuleb kasutada nägemisnurka piiravaid ekraanifiltreid.
7. Tuleb järgida "puhta laua" ja „puhta ekraani“ põhimõtet.

TRM-3 (ülisalajase info töötlemisega seotud ruumid)

8. Peab olema tagatud, et elektrisüsteemi väljalülitumisega ei kaasne infosüsteemi toite kohene kadumine ning sellest tingitult andmete hävimine (st nõutav katkematu toite olemasolu).

4.2.7. Serveriruumid (SRM)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Serveriruumid		SRM-1	SRM-2	SRM-3		SRM-1	SRM-2	SRM-3				SRM-4		SRM-1	SRM-2	SRM-3

SRM-1 (asutuste serveriruumid; asutuste telefonijaama ruumid, milles paiknevaid seadmeid kasutatakse ainult oma asutuse teenindamiseks ja neis ei ole transiitjaamu)**.**

1. Serveriruumid peavad vastama juhtkonna poolt kinnitatud turvaeeskirjadele ja standarditele.
2. Infosüsteemide serverid peavad paiknema nendes töödeldava info turvaklassi nõuetele vastavas turvaalas.
3. Serveriruumides on söömine, joomine ja suitsetamine keelatud.
4. Peavad kehtima protseduurid, mis tagavad, et kui infosüsteemide ekspluatatsiooniga otseselt mittetegelevad isikud peavad sisenema arvutiruumidesse, saadab neid IT osakonna töötaja. Saatjateta pääseb serveriruumi ainult selleks volitatud IT personal vastavalt “Serveriruumi pääsevate IT isikute nimekirjale”, mille kinnitab asutuse juht.
5. Protseduuriliselt peab olema kindlustatud, et kõik infosüsteemide serverid omavad nähtavat märgistust, mis näitab ära serveri nime ja inventarinumbri. Serveriruumis peab olema nimekiri, kus on kirjas serverite nimed koos inventarinumbri, IP aadressi, rakenduse(te), administraatori(te) nime(de) ja nende kontaktandmetega.

6. Peab olema tagatud, et elektrisüsteemi väljalülitumisega ei kaasne andmete hävimist - st sisuliselt nõutav katkematu toiteallikas (UPS), mis garanteeriks vähemalt 15 minutilise varustamise elektriga.
7. Peab toimima pidev serveriruumi temperatuuri kontroll.
8. Peab olema tagatud ruumi jahutus (konditsioneerid), kui temperatuur ei püsi +15 - +25 °C juures.
9. Peab pidama serveriruumi külastajate päevikut.

SRM- 2 (asutuse serveriruum, kus hoitakse andmekogu(sid), milles töödeldakse delikaatseid isikuandmeid. Telefonijaama ruum, kus on transiitjaam).

10. Peab olema tagatud, et infotehnoloogia ekspluatatsioonikoht oleks silmatorkamatu ning selle füüsiline märgistus piiratud.
11. Perioodiliselt tuleb kontrollida ja ajakohastada tehnovõrkude vajadustele vastavust ning - dokumentatsiooni
12. Puuduste/probleemide ilmnemisel peab toimuma kohene tehnovõrkude täiustamine/kontroll ning vastava dokumentatsiooni kaasajastamine.
13. Seadmetel, mis kuvavad või väljastavad informatsiooni loetavas vormis, ei tohi olla ligipääsu volitamata isikutel nii, et nad saaksid neilt lugeda informatsiooni ilma süsteemiadministraatori teadmiseta/loata.
14. Serveriruumis ei tohi olla otseselt mittevajalikke ruumi läbivaid vee-, elektri- jms juhtmeid.
15. Serveriruumi uks peab olema tule ja ründe kindel.
16. Ruumis peavad olema suitsuandurid ja tulekahjusignalisatsioon.
17. Peab olema tagatud, et elektrisüsteemi väljalülitumisega ei kaasne andmete hävimist - st sisuliselt nõutav katkematu toiteallikas (UPS), mis garanteeriks vähemalt 30 minutilise varustamise elektriga.
18. Tuleb säilitada kõigi serveriruumis viibinute logi, kusjuures viibinu autenditakse allkirjaga, näpujäljega, elektroonse võtmekaardiga vms.

SRM- 3 (asutuse serveriruum, serveriruum, milles töödeldakse salajast infot, asutuse telefonijaama ruum).

19. Üleminek teisele toiteallikale toimub süsteemi poolt määratud nõuete kohaselt (nõutav katkematu toiteallikas (UPS) ja generaator.
20. Vajadusel peavad olema kohaldatud meetmed elektromagnetkiirguse põhjal konfidentsiaalse info tuvastamise ja elektromagnetrünnete raskendamiseks/välistamiseks.
21. Ruumis peab olema automaatne tulekustutussüsteem.
22. Peab olema tagatud ruumi jahutus (konditsioneerid).
23. Peavad olema paigaldatud veeandurid.
24. Peab toimuma pidev toite monitooring.
25. Serveriruumi külastajate päevikut/logi tuleb regulaarselt läbi vaadata.
26. Elektroonsel kujul olev info on ainult sisemiseks kasutamiseks ning salajase info ilma erivajaduse ja vastava eriloata turvaperimeetri piiridest väljaviimine on keelatud.

27. Missioonikriitilist infotehnikat sisaldavatest ja ülisalajase info töötlemisega seotud ruumidest elektroonse info väljaviimiseks peavad olema kinnitatud spetsiaalsed korrad ja väga piiratud inimeste nimistu; erijuhtudeks vajalik ettevõtte tippjuhtkonna eriluba.

SRM-4

28. Peaseveriruum ning selles paiknevad missioonikriitiliste rakenduste serverid ja sideseadmed peavad olema dubleeritud.
29. Dubleeriv peaserveriruum peab (soovitavalt) paiknema vähemalt 5. km kaugusel peaserveriruumist.

INFOTEHNOLOOGILISED VAHENDID

4.2.8. Pääsuõigused (PÕ)

Ennekõike tuleb rõhutada, et Pääsuõigused on turvameede, mis vägagi oluliselt kuulub ka Turvaorganisatsiooni tegevusvaldkonda, sest seal määratletakse konkreetsetele infovaradele valdajad/vastutajad. Tegelikult määratlevad valdajad infosüsteemi lubatud kasutajad ja nende õigused. Infotehnoloogiliselt tagatakse ainult valdajate soovide täitmine ja selle kontroll.

Pääsuõiguste realiseerimismehhanism peab võimaldama spetsifitseerida kasutajaid (kasutajate, kasutajate gruppide, avaliku kasutaja pääsuõiguste nimekirjad, kasutaja all tuleb mõista ka infotöötlusprotsessi) ja reguleerida ressursside (nt andmebaasitabelid, failid, programmid, protsessid, seadmed) jaotamist kasutajate, kasutajagruppide või mõlemate vahel.
Pääsu reguleerimine koosneb kahest eraldi vaadeldavast poolest:

- kasutajate autentimine ja
- volitamine ehk autoriseerimine ehk õiguste andmine.

Vastavalt sellele on otstarbekas jagada pääsuõiguste nõuded kaheks eraldiseisvaks nõuete komplektiks.
Pääsuõiguste reguleerimist tuleb vaadelda vähemalt kahel tasemel: operatsiooni-süsteemi tase (süsteemitase) ja rakenduse kasutajaliidese tase (rakenduste tase). Süsteemitaseme pääsu reguleerimine loob rakenduste jaoks keskkonnad, mille piires rakendusprogrammid saavad üles ehitada oma pääsu reguleerimise mehhanismid. Näiteks veebiteenuse osutamiseks pannakse käima protsessid, mis töötavad süsteemitasemel piiratud kasutajaõigustega. Veebiteenust osutavas rakendusprogrammis võidakse omakorda autoriseerida teenuse lõppkasutajad ja anda juurdepääsuõigused konkreetse kasutaja jaoks lubatud objektidele. Rakenduste tasemel antavad õigused on taandatavad mingile alamhulgale teenust osutava protsessi süsteemitaseme õigustest.
Süsteemitaseme õiguste puhul on enamuses kasutusel olevates operatsiooni-süsteemides oluliseks erisuseks eriõigustes kasutaja olemasolu, kellele ei laiene süsteemsed õiguste piirangud (root, administrator, superuser, supervisor, system).
Järgnevates nõuetes tähistab mõiste "pääsu reguleerimine", kui taset pole täpsustatud mõlemat - nii süsteemi- kui rakendustaset.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Pääsuõiguste haldus	PÕ-1	PÕ-2	PÕ-3	PÕ-4	PÕ-1	PÕ-2	PÕ-3	PÕ-4						PÕ-2	PÕ-3	PÕ-4

PÕ-1 nõuded – ei midagi spetsiaalset , ainult opsüsteemiga/rakendusega kaasatulev

1. Objektid peavad olema klassifitseeritud (määratud nõutav/aktsepteeritav turvatase) ning selle vastavalt määratakse neile pääsuõigusi.

2. Personalihaldus ja IT juhtkond peavad tagama asjakohase ja õigeaegse pääsuõiguste muutmise infosüsteemide kasutajate ja IT personali teisele töökohale üleviimiste ja asutusest töölt lahkumiste puhul.

Autentimisnõuded

Kasutajate autentimiseks kasutatakse tunnuseid, mis reeglina koosnevad kahest osast: avalik tunnus (näiteks kasutajanimi) ja salajane tunnus (parool, PIN-kood).

3. Pääsuõiguste süsteem peab tagama, et inforessursid on kaitstud volitamata juurdepääsu eest.
4. Piisavad on kasutajate grup(p)i(de)le omistatud ühised kasutajatunnused ja paroolid. Võib rakendada ka tugevamaid pääsukontrooli meetmeid, kui see ei too kaasa lisakulutusi (nt riistvaraliste tõendite näol).

Volitamis-/autoriseerimisnõuded

5. Pääsuõigusi inforessursile võib anda ainult nõutava vormistatud/kinnitatud taotluse alusel selleks määratud volitatud isik – üldjuhul info valdaja.

PÕ-2 nõuded.

6. Ei tohi anda juurdepääsu enne volitusprotseduuride lõpuleviimist.
7. Kasutajad tuleb kohustada ajutisi paroole vahetama koheselt esimesel sisselogimisel.
8. Vältimaks paroolide sattumist valedesse kätesse tuleb vältida nende talletamist arvutisüsteemidesse kaitsmata kujul.
9. Peab asendama tarkvara väljatöötajate poolt loodud vaikimisi kasutajad ja nende paroolid koheselt pärast tarkvara installeerimist.
10. Kolmandatele osapoolte töötajatele ei tohi anda juurdepääsu informatsioonile ega infotöötlusvahenditele, enne kui on evitatud asjakohased turvameetmed ja alla kirjutatud leping, mis määratleb ühenduse või juurdepääsu tingimused (tuleb selgelt määratleda ja dokumentaalselt fikseerida konfidentsiaalsele infole juurdepääsud).

Autentimisnõuded

11. Kõigil kasutajatel peavad olema isiklikud kasutajatunnused ja korduvkasutusega paroolid.
12. Kasutajate informeerimine: kõiki infosüsteemi volitatud kasutajaid peab enne süsteemi juurdepääsu teavitama sellest, et süsteemi kasutamist jälgitakse, salvestatakse ning see on auditeerimise subjektiks. Kasutaja peab olema teadlik, et süsteemi volitamata kasutamine on keelatud ning et keelu eiramisel võidakse algatada distsiplinaarjuurdluse kasutaja suhtes. Kui süsteem võimaldab, siis iga algne ekraanipilt (kuvatakse enne süsteemi sisenemist) peaks sisaldama kasutajat hoiatavat teksti (esitatud peab olema informatsioon tegevuste jälgimise, salvestamise ja kontrolljälje kohta). Selle teksti kõrvaldamiseks ekraanilt peab kasutaja läbi viima kinnitava tegevuse.
13. Pääsuõiguste kontrolli süsteem (Access Control System) peab võimaldama alljärgnevat:
    (a) limiteerida juurdepääsu katsete arvu teatud aja jooksul - korduvatele katsetele (näiteks 5 korda) kasutada arvutivõrgu või rakenduse kasutajakontot ilma volituseta (vigane kasutajanimi või parool) reageerib arvutivõrgu süsteem või infosüsteem kasutajakonto lukustamisega,
    (b) erijuhtudel (kui juurdepääsu katsete arv pole limiteeritud) kasutada

kontrollsüsteemis viivitust või muid sarnaseid meetodeid (kinnitatuna andmeturbejuhi poolt);

(c) süsteem peab võimaldama sisse logida ainult kooskõlas vastava kasutaja autentimisprofiili (määratud üldjuhul ametikohaga, erijuhtudel veel ka konkreetsele persoonile lubatud tegevustega) tingimustega. Kui täpseid tingimusi ei ole defineeritud, peavad süsteemi sisenemisel olema vaikimisi keelatud kõik kaugtoimingud ja anonüümsed pääsuõigused,

(d) koos kasutaja identifitseerimisega peab toimuma ka kasutaja PC/terminali identifitseerimine;

(e) peab olema tagatud kohustuslik paroolivahetus näiteks iga 90. päeva järel (nõuda seda kasutajatelt, kui pääsuõiguste süsteem ise ei taga);

(f) välistada eelnevalt kasutatud paroolide taaskasutamist (mälus ajalugu näiteks 3'st viimasest),

(g) kehtestada ja kontrollida parooli minimaalset pikkust (näiteks 6 sümbolit).

14. Kaugjuurdepääsu puhul peab rakendama riistvaralist tõendit (n PIN-kalkulaatorit, ID kaarti vms) ja (kui ühendusmeetod võimaldab) ka tagasihelistamist.

Volitamis-/autoriseerimisnõuded

15. Pääsureguleerimine peab defineerima ja reguleerima pääsuõigused kõigi kasutajate ja kõigi inforessursside vahel – st tagab, et pääsureguleerimise subjektidel on võimalik pöörduda üksnes volitustele vastavate objektide poole ja tegutseda vastavalt volitustele (kas lugeda, kirjutada(lisada/muuta) või käivitada).

16. Pääsu reguleerimine peab infot kaitsma volitamata pöördumiste (konfidentsiaalsuse tagamine) ja muutmiste (tervikluse tagamine) eest.

17. Peavad olemas olema dokumenteeritud protseduurid ja tehnilised süsteemi võimalused, mis tagavad, et muudatusi andmetesse teostavad ainult selleks volitatud isikud või andmetöötlusprotsessid.

PÕ-3

18. Tuleb määratleda pääsuõigused salajastele ja ülisalajastele raportitele, konfidentsiaalset informatsiooni käsitlevale dokumendile omavad juurdepääsu vaid volitatud isikud.

19. Tuleb luua kord, millele vastavalt tekitatakse ja hoitakse ajakohasena teatud kindlale konfidentsiaalsele infole juurdepääsuks volitatud gruppide nimistud.

20. Sunni alla sattuda võivatele kasutajatele tuleb luua sunnialarmi võimalus. Otsus sellise alarmi rakendamise kohta peab põhinema riskide hindamisel. Sunnihäirele reageerimiseks peavad olema määratletud kohustused ja protseduurid;

Autentimisnõuded

21. Kõigil kasutajatel peavad olema isiklikud kasutajatunnused ja ühekordsed paroolid (PIN-kalkulaator, paroolilist) või parool, mille muutmist nõutakse regulaarselt (kasutajatel ja administraatoriõigustes kasutajatel iga 45 päeva järel ning administraator ja root paroolidel 1 X aastas). Kehtestada ja kontrollida parooli minimaalset pikkust (kasutajatel ja administraatoriõigustes kasutajatel 8 sümbolit ning administraator ja root paroolidel 12 sümbolit) ja keerukust (suur- ja väiketähed, numbrid, erisümbolid).

22. Peab olema välistatud eelnevalt kasutatud paroolide taaskasutamine (mälus ajalugu 10'st viimasest).

23. Iga positiivse või negatiivse autentimise korral registreeritakse aeg, kasutajanimi,

soovitud õigused ja juurdepääsutee.

24. Vaikimisi võib lubada ainult ühekordset seanssi. Kui infosüsteem lubab mitmekordset sisselogimist peab olema võimalik kontrollida iga kasutaja ID sessioonide või sisenemisi ainult ühelt IP-aadressilt (sisuliselt kindlalt PC-lt teadaolevast/kindlast ruumist).

25. Kui infosüsteem võimaldab, tuleb kontrollida teatud intervalli tagant kasutaja tegevusetust ning keelata edasised toimingud kuni kasutaja on ennast uuesti identifitseerinud. Kasutaja deaktiviseerimine, tegevusetuse periood (n 10 minutit) ja uuesti identifitseerimise (n nõutav parooli uuesti sisestamine) nõuded peavad olema dokumenteeritud.

26. Kui infosüsteem võimaldab tuleb kasutajat teavitada viimas(t)est õnnestunud sisselogimis(t)est (kuupäev ja kellaeg), sisseloginud kasutaja asukohast ja selle kasutaja ID eelnenud ebaõnnestunud logimiskatsete arvust.

27. Kaugjuurdepääsu üksikjuhtudeks on vajalik otsese ülemuse ja andmeturbejuhi luba.

28. Paroolimurdmise spetsiaaltarkvaraga peab perioodiliselt (kord kuus) kontrollima kasutajate paroolide keerukuse piisavust.

Volitamis-/autoriseerimisnõuded

29. Kasutaja autentimisprofiili muutumisel peab pääsureguleerimine tagama kõigi õiguste uuesti määramise kõigi objektide suhtes, millele kasutajal on otseselt või kaudselt juurdepääs.

30. Peavad olemas olema dokumenteeritud protseduurid ja tehnilised süsteemi võimalused, mis tagavad sisestatud andmete tervikluse kontrolli.

31. Peab olema tagatud kõigi pääsu reguleerimisega seotud tegevuste ja nende käigus teostatud muudatuste logimine (Windows'is/Unix'is/Linux'is olemas, rakendustesse peab olema sisse programmeeritud).

32. Kasutajal peab olema võimalik soovi korral esitada süsteemile päringut oma kasutajaõiguste kohta raporti saamiseks.

Lepingunõuded

Lisaks autentimis- ja volitamisnõuetele tuleb sisse tuua pääsu reguleerimise mehhanisme ja organisatsioonilisi meetmeid ühendavad nõuded, mis peavad kajastuma kasutajatega sõlmitavate lepingutes.

33. Muutmisõigusega kasutajaga sõlmitud lepingus (teenuseleping, tööleping vmt.) peab sisalduma salajaste autentimistunnuste saladuses hoidmise kohustus ja tunnuse avalikustumise korral partneri viivitamatu teavitamise kohustus.

PÕ-4

Autentimisnõuded

34. Kõigil kasutajatel peavad olema isiklikud kasutajatunnused (isiklik kasutajanimi ja parool, mille muutmist nõutakse regulaarselt) ja riistvaralised ja/või biomeetrilised tõendid.

35. Peab olema kehtestatud ja kontrollitav parooli minimaalset pikkust (12 sümbolit) ja keerukust (suur- ja väiketähed, numbrid, erisümbolid).

36. Kasutades FT-2 tasemel füüsiliselt turvatud ja eelnevalt fikseeritud arvutit/terminali võib kasutaja ennast autentida ka PÕ-2 tasemele vastavalt.

37. Peab rakendama reaalajas töötavat ebaõnnestunud autentimiste kontrolli ja alarmsüsteemi.

38. Kaugjuurdepääs on keelatud.

Volitamis-/autoriseerimisnõuded

39. Pääsureguleerimine peab võimaldama spetsifitseerida igale nimetatud ressursile isikute ja/või isikute gruppide nimekirja, kellel ei ole pääsuõigust nimetatud ressursile. (Traditsiooniline lubamis-põhine pääsureguleerimise võimalus on iseenesestmõistetavalt primaarsena/paralleelsena ka olemas ja kasutuses. Üldjuhul eeldab spetslahendust, sest tavaliselt ACS'id seda ei võimalda, kuid on välja ilmunud ka esimene pääsuke – NSA SE Linux.)

Lepingunõuded

40. Salajastele ja eriti salajastele objektidele ligipääsu omavate kasutajatega sõlmitud lepingus peab kajastuma salajaste ja eriti salajaste andmete saladuses hoidmise kohustus ja partneri viivitamatu teavitamise kohustus andmete avalikustumise korral.

4.2.9. Side (KOM)

Küllalt tihti on mõttekas kasutada mingi kõrgete turvanõuetega missioonikriitilise infosüsteemi jaoks vajalikke ja juba juurutatud/juurutatavaid turvalahendusi ka vähemkriitiliste juures. Ja side on väga sobilik koht eelneva mõtte järgimiseks - ei tekita olulisi lisakulutusi, sest teised infosüsteemid lihtsalt kasutavad mingit juba olemasolevat turvalahendust. Seega turvanõuded sidele on üldjuhul määratletud kõige missioonikriitilisema rakenduse/infosüsteemi nõuetega.

Informatsiooni edastamisel tuleb tagada sellele pääsuõigustega määratletud kontrollitud juurdepääs. Tuleb rakendada adekvaatseid meetodeid, et tagada info kaitstus isikute eest, kellel juurdepääs ei ole lubatud.

Traditsiooniliselt kasutatakse asutuste perimeetri kaitseks näiteks ruutereid (access list), tulemüüre (packet-/content filtering), proxy'sid/socks'id, võrgu- ja serveripõhist rünnete tuvastamist (Intrusion Detection/Avoidance Systems), VPN (krüpteeritud ühendused üle ebaturvaliste sideliinide) ja viirusetõrjet.

Parim tulemus saavutatakse üldiselt mitmetasemelise infoturbega, kus uued proaktiivseid (tegevuspõhised) turvalahendused on kasutusel koos traditsiooniliste tehnoloogiatega (signatuuripõhine viiruste-, reklaam-,nuhk- ja õelvara avastamine/tõrje; Internetikasutuse kontroll/URL-filtreerimine).

Edaspidise käsitluse loogika seisukohalt on sideühendused/infovahetus jagatavad kaheks infoturbe seisukohalt küllalt erinevaks tüübiks/tasemeks ning neid käsitletakse detailsemalt kahes järgnevas allteemas (VPK ja SVT):

- välisühendused ettevõtte sisevõrku (WAN, Internet, telefoniliinid/eraldatud liinid, spetsiaalvõrgud –n SWIFT, Reuters jne)– käsitletakse VälisPerimeetri Kaitse (VPK) allteemas,
- informatsiooni levitatakse/edastatakse ainult sisevõrgus, kus puuduvad võrguarhitektuurilised piirangud infovahetuseks – SiseVõrgu (LAN/Intranet) Turve (SVT) allteema.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Side	KOM-1	KOM-2	KOM-2	KOM-3	KOM-1	KOM-2	KOM-2	KOM-2					KOM-1	KOM-2	KOM-2	KOM-3

KOM-1

1. Tagada ühenduste toimivus (nii sisevõrgus kui ka välisühendustel): jälgida ühenduste koormatust, probleemsete olukordade diagnostika/analüüs, rakendada meetmed mittevajalike andmevoogude osakaalu vähendamiseks/vältimiseks, mittesoovitud andmevoogude allikate blokeerimine.
2. Sideseadmed peavad tagama häirete tõttu tekkinud vigade avastamise ja soovitavalt ka parandamise.

KOM- 2

3. Informatsiooni füüsiliseks edastamiseks kasutatakse usaldusväärset kullerit ja rakendatakse meetmeid saadetise kopeerimise-vahetamise vältimiseks (saadetis paigutatakse turvakotti, elektroonilised andmekandjad šifreeritakse jne.).
4. Transpordi usaldusväärsuse tagamiseks peab olema evitatud volitatud kullerite loetelu, mis tuleb kokku leppida juhtkonnaga ja juurutada vastav protseduur kullerite identiteedi kontrolliks.
5. Tuleb nõuda kokkulepitud märgistuse kasutamist salajase või ülisalajase informatsiooni puhul, nii et see tagab märgendite viivitamatu mõistmise ja informatsiooni asjakohase kaitse.
6. Lokaalvõrgus andmeedastuseks kasutatavad magistraalkaablid peavad olema kaitstud pealtkuulamise ja tahtliku hävitamise eest (eeldavad füüsilist juurdepääsu).
7. Kõik välisühendused asutuse sisevõrgu ressurssidele peavad olema tehtud läbi turvalisust tagava pääsukeskkonna (ruuter või tulemüür), otsesed välisühendused sisevõrku on keelatud (näiteks modemite/modemiühenduste kasutamine sisevõrgus/sisevõrku keelatud, otsene juurdepääs Internetist ja välispartnerite võrkudest keelatud jne).
8. Kõik ühendused Internetist ja välispartnerite võrkudest peavad olema termineeritud DMZ's paiknevas proksis, socksis või muud funktsiooni kandvas serveris.
9. Kaugjuurdepääs: peab kasutama kaugjuurdepääsu turvalisust tagavaid infotehnoloogilisi lahendusi (VPN, asutuse keskne sissehelistamiskeskus), autentimiseks kasutada ühekordseid paroole ja (kui ühendusmeetod seda võimaldab) kasutada ka tagasihelistamist.

KOM- 3

10. Kõik välisühendused sisevõrku peavad olema tehtud läbi turvalisust tagava ja vähemalt kolmetasandilise pääsukeskkonna (väliskeskkond -> tulemüür -> DMZ -> tulemüür -> sisevõrk).
11. Kaugjuurdepääs: peab kasutama kaugjuurdepääsu turvalisust tagavaid infotehnoloogilisi lahendusi (VPN, asutuse keskne sissehelistamiskeskus), autentimiseks kasutada riistvaralist tõendit (n PIN-kalkulaatorit, ID kaarti vms) ja (kui ühendusmeetod seda võimaldab) kasutada ka tagasihelistamist.
12. Sundtee: infosüsteem peab määratlema (peale kasutaja identifitseerimist ja autentimist) sundtee ressursi ja kasutaja vahel. Sundtee peab tagama, et usaldamatu protsess ei saa kinni püüda või modifitseerida kasutaja ühendust.
13. Terviklus: adekvaatse informatsiooni edastamiseks peab kogu edastatav informatsioon sisaldama konfidentsiaalsuse ja tervikluse tagatuse atribuute.

KOM- 4

14. Kõik välisühendused sisevõrku peavad olema tehtud läbi turvalisust tagava ja vähemalt viietasandilise pääsukeskkonna (väliskeskkond -> filtreeriv ruuter ja tulemüür -> DMZ -> filtreeriv ruuter ja/või tulemüür -> sisevõrk) ning peaks olema võimalik DMZ ümberstruktureerimine loogiliselt üksteisest eraldatud alamDMZ-deks.
15. Kõik olulised välisühendused peavad olema dubleeritud – ringlahendused, sideteenused alternatiivsetelt sideteenuse pakkujatelt vms.

4.2.10. Välisühenduste ja Välisperimeetri Kaitse (VVK)

Välisperimeetri kaitse all mõistame välismaailma ja asutuse sisevõrku eraldava joone (välisperimeetri) korrektset määratlemist ning selle edasist rünnete/õelvara jms vastast kaitset.

Sisuliselt häkkerite/kräkkerite ja ka muu õelvara (adware, spyware, malware) poolt väga erinevatel eesmärkidel sooritatavate rünnete ja selle käigus kasutatava tarkvara volitamatu laadimise/käitamise tuvastamine, teavitamine ja kaitse.

Ka välisperimeetri kaitsel on mõttekas kasutada mingi kõrgete turvanõuetega missioonikriitilise infosüsteemi jaoks vajalikke ja juba juurutatud/juurutatavaid turvalahendusi ka vähemkriitiliste juures - ei teki olulisi lisakulutusi, sest teised infosüsteemid lihtsalt kasutavad mingit juba olemasolevat turvalahendust.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Välisperimeetri ja Välisühenduste Kaitse		VVK-1	VVK-2	VVK-3		VVK-1	VVK-2	VVK-3						VVK-1	VVK-2	VVK-3

VVK-1

1. Kõik välisühendused peavad sisevõrgust olema eraldatud ruuteri või tulemüüriga.
2. Peavad olema dokumenteeritud ja rakendatud tulemüüri läbipääsu poliitika/põhimõtted nii seadmete, kasutajate grupi kui ka kasutajate tasemel.
3. Tagada välisühenduste toimivus: välisühenduste diagnostika/analüüs, rakendada meetmed mittevajalike andmevoogude osakaalu vähendamiseks/vältimiseks, mittevajalike andmevoogude allikate blokeerimine.
4. Välisühenduste kontroll: välisühenduste kaudu laekuv ja sisevõrgust väljastatav informatsioon tuleb üle kontrollida, otseselt mittevajalikud ühendused tuleb keelata - üldjuhul keelatud ftp, telnet jms; info ei tohi sisaldada viiruseid ega ründeprogramme, meilimanuse kasutuseelne kontroll ründetarkvara avastamiseks.
5. Võrgu tasemel peab olema tagatud: kasutajate/kasutajate gruppide interneti kasutamise kontroll (URL filtreerimine).
6. Kaugtöökohtades tuleb kasutada varunduse ja äritegevuse katkematuse tagamiseks spetsiaalseid protseduure - näiteks rakendada nende töökohtade seiret.

VVK- 2

7. Juurdepääsupiiranguga infot sisaldavate rakenduste serverid peavad olema kaitstud nii välis- kui ka sisekasutajate ebasihipärase tegevuse eest kolmetasemelise kaitsega: Laivõrk -tulemüür-DMZ-tulemüür-Sisevõrk.
8. Välisperimeetri turvalisuse perioodiline testimine (Penetration Testing, Vulnerability Scanning).

9. Peab olema rakendatud ründetuvastuse (IDS) või rünnete tõkestamise (IDA) süsteem.
10. Ühenduste krüpteerimine: kõigi salajase infoga tegelevate rakenduste infoedastuskanalites (klient-rakenduse server) liikuv info (sealhulgas ka autentimis/autoriseerimisinfo) peab olema krüpteeritud üldiselt turvaliseks tunnistatud krüpteerimismeetodiga.
11. Kaugjuurdepääs: peab kasutama kaugjuurdepääsu turvalisust tagavaid infotehnoloogilisi lahendusi (VPN, sissehelistamiskeskus), autentimiseks kasutada ühekordseid paroole ja (kui ühendusmeetod seda võimaldab) kasutada ka tagasihelistamist.

VVK- 3

12. Kontrollpunkt paljude samaaegsete sisevõrgust -> välisvõrku ühenduste (põhiliselt Internetti pöördumistel) turvalisuse parandamiseks/administreerimiseks: kasutada puhverserverit (proxy) – välisliiklust vahendavat tulemüüri komponenti, mis tekitab paljudele välisühendustele ühe punkti, nn *SinglePoint_of_Security,* ning võimaldab:
    - teenuste (ftp, telnet jne) administreerimiste (lubamine/keelamine) - firma võib oma töötajatele ära keelata teatud veebiteenuste kasutamise;
    - päringute filtreerimist - firma võib oma töötajatele ära keelata teatud veebilehekülgede ja uudisgruppide külastamise;
    - suurendab välisühenduse efektiivsust, sest kord puhverserveri vahepuhvrisse loetud info korduvaks lugemiseks otse kättesaadav (st ilma välisühendust kasutamata/koormamata)
    - proksis tehtav NetworkAddressTranslation suurendab turvalisust – sisevõrgu arvuti reaalne IP-aadress pole välisvõrgust nähtav/pöördutav
13. Kaugjuurdepääs: peab kasutama kaugjuurdepääsu turvalisust tagavaid infotehnoloogilisi lahendusi (VPN, asutuse keskne sissehelistamiskeskus), autentimiseks kasutada riistvaralist tõendit (n PIN-kalkulaatorit, ID kaarti vms) ja (kui ühendusmeetod seda võimaldab) kasutada ka tagasihelistamist.
14. Missioonikriitiliste rakenduste serverid peavad olema kaitstud nii välis- kui ka sisekasutajate ebasihipärase tegevuse eest viietasemeline kaitsega : Laivõrk(Välisühendused-telefoniliinid,Internet,eriühendusedSWIFTnäiteksjms)-ruuter-tulemüür-DMZ-tulemüür-ruuter-Sisemine kohtvõrk, DMZ jagamine alamDMZ'deks.
15. Perioodiliselt testida/jälgida serverite ja rakenduste turvalisust välisperimeetril – kasutajate identifitseerimise, teenuste/pöördumiste õiguste ja muude ohtude puhul turvalisuse tagatuse kontrollimine ja juhtimine.
16. Kontrollpunkt paljude samaaegsete Internetipõhiste e-rakenduste klientide välisvõrgust (Internetist) sisevõrku e-rakenduste rakenduste serverite poole pöördumiste turvalisuse parandamiseks/administreerimiseks: pöördproksit (ümberpööratud puhverserver - ReverseProxy) – väljast -> sisse suunatud infoliikluse turvalisust tõstvat komponenti, mis tekitab paljudele väljast->sisse ühendustele ühe nn *SinglePoint_of_Security*:
    - pöördproksi on rakendustaseme lüüsisõlm/värav (ApplicationLayerGateway), mis tekitab kontrollpunkti (SinglePoint_of_Security) veebirakendustele suunatud rünnete vastu (FW ja IDS siin ei aita): väljast palju kliente pöördub ühte IP portti -> ReverseProxy -> üks või mitu veebiserverit/ üks või mitu veebirakendust.

- parandab veebiserveri turvalisust - raskendab tunduvalt veebiserveri mitteturvalisus(t)e (turvaaukude exploit'ide) ärakasutamist, sest häkker ei näe otseselt veebiserverit, selle tüüpi/versiooni,
- vähendab DoS rünnete mõju
- võimaldab veebiserverite koormuste jaotamist, näiteks ka rakenduste lõikes jaotamist
- vahetab lennult URI/URL'i – st internetist pöördutakse ühele URL'ile ning ReverseProxy suunab edasi hoopis teise(te)le sisemise(te)le aadressidele

17. Kogu avaliku võrgu/oluliste avalike serverite rünnatavuse testimine (Penetration Test) vähemalt 1x aastas (et pole avatud üleliigseid porte/teenuseid, kasutatavad teenusprogrammid on uuendatud/paigatud, teenusprogrammide installeerimisel/konfigureerimisel pole tehtud vigu, välistatud vaikimisi installeeritavad kasutajad ja rünnet võimaldavad näidisprogrammid jms).

4.2.11. Sisevõrgu Turve (SVT)

Sisuliselt sisehäkkerite ja õelkoodi (*malicious code*) poolt väga erinevatel eesmärkidel sooritatavate rünnete ja selle käigus kasutatava tarkvara volitamatu laadimise/käitamise tuvastamine, teavitamine ja kaitse.

Sisevõrgu turve on kolmas valdkond, kus turvanõuded on üldjuhul määratletud kõige missioonikriitilisema rakenduse/infosüsteemi nõuetega.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
SiseVõrgu Turve	SVT-1	SVT-1	SVT-2	SVT-3	SVT-1	SVT-1	SVT-2	SVT-3					SVT-1	SVT-1	SVT-2	SVT-3

SVT-1

1. Peavad olema välistatud autoriseerimata/pääsuõigusi mitteomavad pöördumised nii serveritesse kui ka kasutajate tööjaamadesse.
2. Rünnete ning volitamatu tarkvara laadimise/käitamise avastamise/tõkestamise protsessid peavad olema dokumenteeritud ja rakendatud.
3. Peavad olema rakendatud rünnete ning volitamatu tarkvara laadimise/käitamise avastamine/tõkestamine opsüsteemide vahenditega (kasutajate õiguste konfigureerimine, logide jälgimine).
4. Spetsiaalsete süsteemiutiliitide (pääsu-, võrgu- ja muud utiliidid, mis võivad olla võimelised mööduma süsteemi- ja rakenduste turvameetmetest) kasutamine peab olema rangelt reguleeritud;
5. Personaalse tarkvara ostmine või arendamine töötaja poolt peab olema piiratud. Kui selline tarkvara on vajalik, peab iga selline installatsioon olema kooskõlastatud otsese juhi ja IT (osakonna) juhiga.
6. Enne tarkvara kasutamist tuleb see võimalike kahjude vältimiseks eelnevalt hoolikalt testida. Võrreldes vabavara ja kommertstarkvara kasutamist, tuleb vabavara puhul rakendus(t)e testimisel/juurutamisel üldjuhul arvestada suurema töömahuga (kulutustega).
7. Infosüsteemide kasutajad peavad olema instrueeritud vajalikest tegevustest ründe ja viirus(t)ega nakatumise/nakatumiskahtluse korral ja on võtnud ka vastava kirjaliku täitmiskohustuse.
8. Mobiilset töökohta soovivad töötajad peavad selleks esitama juhtkonnale avalduse, milles on selgitatud mobiiltöökoha kasutusotstarvet;

9. Mobiilseid töövahendeid kasutavale personalile tuleb korraldada koolitus, teadvustamaks lisariskidest ja rakendutavatest turvameetmetest.

SVT-2

10. Sisevõrgu toimimist ja turvalisust tagavate seadmete ning süsteemide administreerimine peab toimuma tsentraliseeritult.
11. Sisevõrku aeg-ajalt ühendatavad mobiilsed kaugtöökohad (Notebook PC'd, PDA'd) peavad olema turvalised (standardkonfiguratsioonis näiteks tulemüür, antiviirus, salajase/ülisalajase info krüpteerimine, VPN, varukoopia tegemislahendus, konfiguratsiooni turvalisuse säilitamiseks pole kasutajatel administraatori õigusi; tagatud võimalus, erivajadusel ja sisevõrgust eraldatult, mobiilse töökoha turvalisuse kontrolliks).
12. Missioonikriitiliste serverite turvalisuse (haavatavuste/nõrkuste) perioodiline kontroll (eTrust vms): kasutajate ja nende õiguste haldus, potentsiaalselt ohtlike failide olemasolu, failide/kataloogide pääsuhaldus (st opsüsteemide ja baasrakenduste vaikimisi-/näidisinstallatsioonid vms pole tekitanud üldteatud näidis-kasutajanimesid, nende poolt käivitatavaid ja potentsiaalselt ohtlikke koode, õigusi konfidentsiaalset infot sisaldavatele failidele/kataloogidele/andmebaasidele, mittesoovitavaid administreerimisõigusi jne).

SVT-3

13. Infovahetusel Internetis (meil, ftp, http) peab olema tagatud rünnete ja viiruste efektiivne ja kindel tuvastamine enne vastava info kasutajatele (st sisevõrku) edastamist (Content Scanner'id DMZ's jms).
14. Missioonikriitilised süsteemid vajavad spetsialiseeritud (isoleeritud) töötluskeskkonda (sisevõrgu segmenteerimist parema kontrolli ja viiruste/rünnete kaitstuse tagamiseks).
15. Missioonikriitiliste serverite turvalisuse (haavatavuste/nõrkuste) pidev/reaalajas jälgimine, kontroll ja monitoorimine.
16. Volitamata tarkvara avastamise ja jälgimise süsteemi turvakihti tuleb testida vähemalt kord kuus erinevate rünnete avastamise ja jälgimisvahenditega (süsteemid snifferite, paroolikräkkerite, klaviatuuri logijate jms avastamiseks/tuvastamiseks).

4.2.12. Viiruste ja muu õelkoodi rünnete tuvastamine ning tõrje (VÕT)

Sisuliselt viiruste, reklaamvara, nuhkvara ja õelvara (adware, spyware, malware) poolt sooritatavate rünnete ja selle käigus kasutatava tarkvara volitamatu laadimise/käitamise tuvastamine, teavitamine ja kaitse.
Ka viiruste ja õelkoodi rünnete tuvastamine ning tõrje on valdkond (neljas), kus turvanõuded on üldjuhul määratletud kõige missioonikriitilisema infosüsteemi nõuetega.

Aeg, kui missioonikriitilise info kaitse võis usaldada signatuuri-põhisele antiviirustarkvarale, on möödas. Tänaste ohtude/rünnete tõrjeks on vajalik proaktiivne andmeturve, mis võimaldab tuvastada/võidelda ka uute senitundmatute ründekoodidega. Näiteks pakutakse välja efektiivseid lahendusi proaktiivseks võitluseks senitundmatute õelkoodidega - ActiveX, Java, VBScript and JavaScript programmidega, kasutades reaalajas käitumispõhise analüüsi tehnoloogiat, mis ei eelda signatuuride andmebaasi olemasolu ja ajakohasust.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Viiruste ja õelkoodi tuvastamine ning tõrje	VÕT-1	VÕT-1	VÕT-2	VÕT-3	VÕT-1	VÕT-1	VÕT-2	VÕT-3					VÕT-1	VÕT-1	VÕT-2	VÕT-3

VÕT-1

1. Viiruste ning volitamata tarkvara laadimise/käitamise avastamise/tõkestamise protsessid peavad olema dokumenteeritud ja rakendatud.
2. Viiruste ning volitamata tarkvara avastamiseks/tõkestamiseks kasutatakse spetsiaaltarkvara, mis tagab rünnete ja viiruste efektiivse tuvastamise.
3. Võrgus olevatel arvutitel peab viirustõrjevahendile versiooni-uuendusi tegema vähemalt kord nädalas ja arvutitel, mis ei ole võrgus vähemalt kord kuus.
4. Infosüsteemide kasutajad peavad olema instrueeritud vajalikest tegevustest viiruste ja/või volitamata tarkvara nakatumise/nakatumiskahtluse korral ning on võtnud ka vastava kirjaliku täitmiskohustuse.
5. Programmide sisseostmisel tuleb osta (võimaluse korral lähtekoodi kujul) mainekast (tuntud) allikast ja nii et koodi saaks verifitseerida.
6. Enne programmide kasutuselevõttu tuleb kogu kood kontrollida salakanalite/tagauste või trooja-koodi avastamiseks.

VÕT-2

7. Viiruste ning volitamata tarkvara avastamiseks/tõkestamiseks kasutatakse spetsiaaltarkvara, mis tagab rünnete ja viiruste efektiivse tuvastamise ning ründe/viiruse tuvastamisel andmeturbega ja kliendiabiga tegeleva personali automaatse informeerimise (eposti- ja/või SMS-teatega, häire monitooringusüsteemi vms).
8. Arvuti tasemel viiruste ning reklaam-, nuhk- ja õelvara (ad-/spy-/malware) avastamiseks/tõkestamiseks peab kasutama spetsiaaltarkvara versioone, millistel on tagatud (ka kasutajate arvutites) pidev automaatne versiooniuuendus.
9. Infovahetusel Internetis (meil, fail, http) peab olema tagatud viiruste ning volitamata tarkvara efektiivne ja kindel tuvastamine enne vastava info kasutajatele (st sisevõrku) edastamist (Content Scanner'id DMZ's jms).

VÕT-3

10. Viiruste ning volitamata tarkvara laadimise/käitamise avastamisel/tõkestamisel kasutatakse spetsiaaltarkvara, mille konfigureering, pidev versiooni- ja signatuuride andmebaasi uuendus jms protsessid peavad olema dokumenteeritud ja rakendatud.
11. Võrgu tasemel peab olema tagatud: viiruste ja reklaam-, nuhk- ja õelvara võrgupõhine proaktiivne (tegevuspõhine) avastamine/tõrje (n SurfinGate for Web ja SurfinGate for Email).
12. Viiruste ning volitamata tarkvara avastamise ja jälgimise süsteemi turvakihti tuleb testida vähemalt kord kuus erinevate rünnete avastamise ja jälgimisvahenditega.
13. Peab kasutatama samaaegselt vähemalt kahte erinevat üldtunnustatut viiruste ning volitamata tarkvara avastamise/tõkestamise spetsiaaltarkvara versiooni, et tagada suurem kindlus uute viiruste/volitamata tarkvara kaitse

(avastamise/tõkestamise) ajakohasusest (sobiv näiteks ka kui üks neist võrgu tasemel ja teine, traditsiooniline, arvuti-tasemel).

4.2.13. Info krüpteerimine (KR)

Kohustuslikud üldpõhimõtted:

1. Asutuse krüptograafiapoliitika elluviimisel tuleb arvestada eeskirju ja riiklikke kitsendusi, mis võivad maailma eri paigus kehtida erinevate krüptograafiliste meetodite kasutamise kohta. Samuti tuleb arvestada küsimusi, mis on seotud krüpteeritud informatsiooni kulgemisel üle piiride;
2. Mobiiltöövahendites peab konfidentsiaalne info olema krüpteeritud kujul, et välistada informatsiooni lekke riske.
3. Kõigi salajase infoga tegelevate rakenduste infoedastuskanalites (klient-rakenduse server) liikuv info peab olema krüptitud - sealhulgas ka autentimis/autoriseerimisinfo.
4. Ülisalajast infot (krüpteerimisvõtmed, VISA kaardivõtmed, PIN-info, …) tohib säilitada ainult krüptitult spetsiaalriistvaras või turvalises seifis (st seif tulekindel, ruum veekindel).
5. Ülisalajase info kandjate füüsilistel ärastamiskatsetel peab olema tagatud andmekandja ja sellel olevate andmete füüsiline hävinemine.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Info krüpteerimine																
Krüpteerimine		KR-K1	KR-K2	KR-K3												
Pääsukontroll		KR-P1	KR-P2	KR-P3		KR-P1	KR-P2	KR-P3						KR-P1	KR-P2	KR-P3
Tervikluskontroll													KR-T1	KR-T2	KR-T3	KR-T4
Võtmehaldus	KR-V1	KR-V2	KR-V3	KR-V4			KR-V2	KR-V3					KR-V1	KR-V2	KR-V3	KR-V4

Käesolev osa käsitleb lähemalt krüptograafilistel meetoditel põhinevaid andmeturbemeetmeid. Kõik loetletavad meetmed toetuvad omakorda madalama taseme teenustele/infrastruktuurile. Vajalik on krüptograafilisi meetmeid komplekssselt täiendada mittekrüptograafilistega, nt. lisaks krüpteerimisele tuleb sõlmida konfidentsiaalsusnõudeid sisaldavad lepingud kõigi osapoolte vahel. Pääsukontrolli puhul tuleb fikseerida muudatuse tegija ja muudatuse aeg jne. Osade meetmete puhul on oluline, kas neid rakendatakse andmete edastamisel või salvestamisel. Kasutatava metoodika piiratuse tõttu jäävad need eraldi vaatlemata. Enamus rakendusi on jagatud loogiliselt kihtideks. Sobiliku turbemeetmete rakenduskihi valikut siin ei puudutata.

Käsitluse loogilisuse ja ülevaatlikkuse huvides on krüpteerimine jagatud neljaks alamteemaks:
- andmete krüpteerimine
- pääsukontroll
- tervikluskontroll
- võtmehaldus

ANDMETE KRÜPTEERIMINE (eelkõige konfidentsiaalsusnõuete tagamiseks)

Avalikud andmed

6. Krüptograafiliste meetodite rakendamine konfidentsiaalsuse tagamiseks ei ole vajalik.

KR-K1
Andmed sisemiseks kasutamiseks

Nõuded krüpteerimise rakendamisele sõltuvad edastus- ja säilitamiskeskkonnast.

7.	Avalik Internet, DMZ	Andmed peavad olema krüpteeritud. Lubatav nõrgendatud algoritmide kasutamine
8.	Asutuse WAN	Andmed võivad olla krüpteeritud, kui seda on võimalik teha efektiivselt arvutivõrgu transpordikihis
9.	LAN jms	Krüpteerimine ei ole vajalik

KR-K2
Salajased andmed

Nõuded krüpteerimise rakendamisele sõltuvad edastus- ja säilitamiskeskkonnast.

10.	Avalik Internet, DMZ	Andmed peavad olema tugevalt krüpteeritud. Tarkvaralise krüpteerimise puhul peab kasutama dokumenteeritud ning Andmeturbejuhi poolt kinnitatud võtmehaldusprotseduure.
11.	Asutuse WAN, LAN	Andmed peavad olema tugevalt krüpteeritud.
12.	Füüsiliselt eraldatud privaatvõrk	Krüpteerimine ei ole vajalik

KR-K3
Eriti salajased andmed

13. Eriti salajasi krüpteeritud andmeid sisaldavad infotöötlusressursid/infokandjad peavad paiknema vähemalt FT-3 tasemel füüsiliselt turvatavates ruumides.

14. Eriti salajasi krüpteerimata andmeid sisaldavad infotöötlusressursid /infokandjad peavad paiknema vähemalt FT-4 tasemel füüsiliselt turvatavates ruumides.

Nõuded krüpteerimise rakendamisele sõltuvad edastus- ja säilitamiskeskkonnast:

15.	Avalik Internet, DMZ	Eriti salajaste andmete edastamine on lubatud üksnes riistvaralise võtmehalduse korral. Edastuskanali turbemeetmed tuleb kooskõlastada andmeturbejuhiga.
16.	Asutuse WAN, LAN	Andmed peavad olema tugevalt krüpteeritud. Soovitatav on riistvaraline võtmehaldus. Tarkvaraline lahendus koos dokumenteeritud võtmehaldusprotseduuridega tuleb kooskõlastada andmeturbejuhiga.
17.	Füüsiliselt eraldatud privaatvõrk	Andmed peavad olema tugevalt krüpteeritud. Võtmehaldusprotseduurid peavad olema dokumenteeritud.
18.	Seifis säilitatav võrguühenduseta arvuti, riistvaraline seade	Kui krüpteerimist ei kasutata, peavad kõik juurdepääsuviisid olema dokumenteeritud.

PÄÄSUKONTROLL

Kõik siin esitatud nõuded/meetmed kehtivad/sisalduvad ka üldises pääsuõiguste halduses – vt 4.2.8 Pääsuõigused (PÕ).

Pääsukontrolli tagamisel võib vabalt rakendada ka tugevamaid meetmeid, kui see ei too kaasa lisakulutusi. Kui samu pääsutõendeid kasutatakse mitmes erinevas süsteemis, peab rakendama kõige rangemaid nõudeid ühtlaselt kõigis süsteemides.

KR-P1 (Sisalduvad PÕ-2s)

19. Kõigil kasutajatel peab olema isiklik kasutajanimi ja parool.
20. Kaugjuurdepääsu puhul peab rakendama riistvaralist tõendit.

KR-P2 (Sisalduvad PÕ-3s)

19. Kõigil kasutajatel peab olema isiklik kasutajanimi ja parool, mille muutmist nõutakse regulaarselt.
20. Parooli vastavust elementaarsetele keerukusnõuetele kontrollitakse.
21. Iga positiivse või negatiivse autentimise korral registreeritakse aeg, kasutajanimi, soovitud privileegid ja juurdepääsutee.
22. Kaugjuurdepääsu üksikjuhtudeks on vajalik andmeturbejuhi luba.

KR-P3 (Sisalduvad PÕ-4s)

23. Kõigil kasutajatel peab olema isiklik kasutajanimi ja parool, mille muutmist nõutakse regulaarselt.
24. Paroolide keerukust (entroopia vähemalt 60 bitti) kontrollitakse.
25. Peab olema täidetud üks tingimustest:
26. Kasutaja peab ennast eelnevalt autentima P2 tasemele vastavalt
27. Kasutatakse isiklikku riistvaralist tõendit
28. Kasutama peab füüsilisel turvatud ja eelnevalt fikseeritud terminali
29. Riistvaralise tõendi kasutamine on soovitatav.
30. Iga positiivse või negatiivse autentimise korral registreeritakse aeg, kasutajanimi, soovitud privileegid ja juurdepääsutee.
31. Peab rakendama reaalajas töötavat alarmsüsteemi.
32. Otsene kaugjuurdepääs on keelatud.

TERVIKLUSE/TUVASTATAVUSE TAGAMINE

KR-T1

33. Edastus- ja/või salvestusseadmed peavad tagama füüsiliste vms häirete tõttu tekkinud vigade avastamise ja soovitavalt ka parandamise (Sisaldub KOM-1s).

KR-T2

34. Andmete volitamata muutmise vältimiseks tuleb rakendada ühte järgnevast:
    - Vähemalt klassile KR-K2 vastavat krüpteerimist koos tervikluskontrolliga
    - Dokumenteeritud võtmehaldusega MAC-i
    - Leitakse räsi, mis tehakse kõigile osapooltele vähemalt KR-T2 – terviklusklassiga kättesaadavaks

- Digitaalsignatuur

KR-T3

35. Andmete võltsimise vältimiseks tuleb rakendada ühte järgnevast:
    - Riistvaralise võtmehaldusega MAC-i
    - Salgamatu digitaalsignatuur

KR-T4

36. Andmed peavad olema varustatud Eesti Vabariigi Digitaalallkirja seadusele vastava või rahvusvaheliste rakenduste puhul Euroopa Liidu direktiivi 1999/93/EC definitsioonile (DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures) vastava digitaalallkirjaga.

VÕTMEHALDUS

KR-V1

37. Võtmeid tuleb käsitleda kui klassi S1 K2 R1 T2 andmeid

KR-V2

38. Võtmeid tuleb käsitleda kui klassi S2 K2 R2 T2 andmeid.
39. Peab olema määratud vastutav isik.

KR-V3

40. Võtmeid tuleb käsitleda kui klassi S2 K3 R2 T3 andmeid.
41. Peab olema määratud vastutav isik.
42. Võtmehaldusprotseduurid peavad olema dokumenteeritud.
43. Sertifitseerimis- vms. ahelas tipmised võtmed tuleb deponeerida.

KR-V4

44. Võtmeid tuleb käsitleda kui klassi S3 K3 R2 T3 andmeid.
45. Võtmehaldur peab olema määratud.
46. Võtmehaldusprotseduurid peavad olema dokumenteeritud ja andmeturbejuhi poolt kinnitatud.
47. Kõigi tegevuste kohta peetakse päevikut või jääb võltsimatu kontrolljälg..
48. Võtmete säilitamiseks tuleb rakendada spetsiaalriistvara.

4.2.14. Seire (MON)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Seire	MON-1	MON-2	MON-3	MON-4	MON-1	MON-2	MON-3	MON-4	-	-	-	-	MON-1	MON-2	MON-3	MON-4

MON-1

1. Seire sisuliselt puudub. Süsteemide tegevusi jälgitakse operatsioonisüsteemi vahenditega (eritarkvara ei rakendata).

MON-2

2. Peab olema korraldatud erisüsteemide abil kontroll tule, vee, temperatuuri,

niiskuse, elektritoite jmt. häirete üle.

3. Info seire käigus tuvastatud tõrgetest/turvaintsidentidest tuleb edastada logimissüsteemile ja salvestada/arhiveerida.
4. Regulaarne perioodiline kontrolljälje analüüs LogideKeskserveril.
5. Vastutajate informeerimine eposti teel (n kaks korda päevas) saadetavate valveraportitega.

MON-3

6. Vastutajate viivitamatu informeerimine päevastest intsidentidest, öisel ajal toimunud intsidendi korral informeerimine hommikul.
7. Infoteenuste tulemuslikkuse ja klientide rahulolu hindamiseks on vajalik seireandmete kogumine ja analüüs ning ühtlasi ka aruandlus juhtkonnale.

MON-4

8. Vastutajate viivitamatu informeerimine intsidentidest (sõltumata nädalapäevast ja kellaajast).

Mõningad näited monitooritavatest olukordadest/intsidentidest:

(a) Mingi oluline rakendus või protsess ei tööta
(b) Mingi oluline protsess (n varukoopiate tegemine) ebaõnnestus
(c) Sisselogimiste kontrollid: näiteks alarm "parooli skaneerimine" kui 15 ebaõnnestunud sisselogimiskatset ühe ja sama kasutaja ID poolt 15. minuti kestel;
(d) Ressursside kasutamine: näiteks alarm süsteemi ressursside (näit. mälu, kettaruum) ebakorrektsest kasutamisest kui mingi kasutaja/rakendus oluliselt häirib/segab teis(t)e kasutaja(te)/rakenduse(te) juurdepääsu inforessurssidele.

4.2.15. IS kasutajate töö jälgimine (KJ)

Infosüsteemi kasutajate töö jälgimine käsitleb viit tegevuste valdkonda:

1. Sessiooni kontroll - kasutaja identifitseerimise ja autentimise eesmärgil peab kontrollima kasutajaseansi loomist.
2. Tehingute autentimine/autoriseerimine – tehingute/andmete sisestaja/muutja peab omama selleks õigusi ja tema tegevused peavad olema hiljem ka tuvastatavad.
3. Andmete sisestuse ja muutmise kontroll - eesmärgiks on informatsiooni õigsuse/täielikkuse tagamine.
4. Ressursside kasutamine - peab olema võimalik kontrollida süsteemi ressursse (nt mälu, kettaruum) selliselt, et ükski kasutaja/rakendusprogramm ei saaks võimatuks muuta teise kasutaja/rakenduse juurdepääsu inforessurssidele.
5. Kontrolljälg: peab olema tagatud infosüsteemi kasutajate ja administraatorite poolt turvalisuse seisukohalt olulisteks loetud tegevuste informatsiooni salvestamine ja arhiveerimine. Kontrolljälje salvestisi kasutatakse tegevuste ja nende tegevuste eest vastutavate isikute seostamiseks ning vajadusel ka analüüsiks.

Kuna kasutajate autentimise/autoriseerimisega tegeleb põhiliselt pääsuõiguste osa (vt 4.3.8. Pääsuõigused), andmete õigsuse/tervikluse tagamisega spetsiaalsed rakendustesse sisseehitatud kontrollid (vt Info klassifitseerimine) ja ressursside kasutamisega seiresüsteemid (vt 4.3.11. Seire) (ka füüsilise turbe ruumide

elektroonsed pääsusüsteemid tegelevad tegelikult kasutajate töö jälgimisega), siis siin käsitleme kasutajate töö jälgimist lihtsustatult ja ainult kontrolljälje tekitamise/salvestamise/analüüsiga/arhiveerimisega seotud turvameetmeid.

Seega siin ja lihtsustatult: kasutajate töö jälgimine on võrdsustatud kontrolljälje tekitamise/salvestamise/analüüsi/arhiveerimisega.

Kontrolljälg sisaldab informatsiooni infosüsteemi kasutajate ja administraatorite tegevustest. Kontrolljälje salvestisi kasutatakse tegevuste, nende teostajate ja tegevuste eest vastutavate isikute seostamiseks. Salvestatud kontrolljäljed on järgneva analüüsi ja arhiveerimise aluseks.

Võimalikud KJ realiseerimisvariandid (rõhutan veelkord, et lihtsustatult, sest osa teemast/turvameetmetest on käsitletud teistes allteemades) **:**

KJ-1: arvuti opsüsteemi ja rakenduste autonoomne logiteenus/logideemon tekitavad logifailid (opsüsteemidest see teenus olemas kõigil enamkasututel: Windows, Linux, Unix; rakendustel logiteenuse olemasolu küllaltki küsitav); vajadusel logide ülevaatus - seega ei midagi spetsiaalset , ainult opsüsteemiga/rakendusega kaasatulev;
KJ-2: serverid edastavad automaatselt oma opsüsteemide ja kui võimalik ka rakenduste (opsüsteemidest see teenus olemas kõigil enamkasututel: Windows, Linux, Unix; rakendustel logiteenuse olemasolu küllaltki küsitav) autonoomsed logid kesksele logiserverile; logide perioodiline ülevaatus/analüüs;
KJ-3: rakenduste logiteenus nõutav; serverid edastavad automaatselt oma süsteemide/rakenduste autonoomsed logid kesksele logiserverile; keskse logiserveri HA-lahendus (klaster); logide analüüs reaalajas;
KJ-4: keskse logiserveri HA-klasterlahendus, rakendus lisab klientide automaatselt keskserverile edastatavatele logidele nii kliendi kui keskserveri digitaalallkirjad ja ajatemplid, reaalajas toimiv logide analüüsi- ja teavitamissüsteem.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS kasutajate töö jälgimine	KJ-1	KJ-2	KJ-3	KJ-4	KJ-1	KJ-2	KJ-3	KJ-3	-	-	-	-	KJ-1	KJ-2	KJ-3	KJ-4

KJ-1

1. Tuleb pöörata tähelepanu logimisvahendi enda turbele, et vältida logifailide muutmist või kustutamist.
2. Automaatse kontrolljälje loomine: infosüsteem loob automaatselt kontrolljälje või vastavasisulise logi (opsüsteemidest see teenus olemas kõigil enamkasututel: Windows, Linux, Unix; rakendustel logiteenuse olemasolu küllaltki küsitav).
3. Peab olema tagatud infosüsteemi kasutajate ja administraatorite poolt turvalisuse seisukohalt olulisteks loetud tegevuste informatsiooni salvestamine ja arhiveerimine. Kontrolljälje salvestisi kasutatakse tegevuste ja nende tegevuste eest vastutavate isikute seostamiseks.
4. Kasutajatelt saadud teated info- ja sidesüsteemide tõrgetest/turvaintsidentidest tuleb edastada logimissüsteemile (ja

salvestada/arhiveerida).

5. Kontrolljälje turve: kontrolljälg peab olema kaitstud volitamata juurdepääsu, muutmise või kustutamise eest.
6. Kontrolljälje analüüs: vastavalt vajadusele.
7. Tõrgete käsitluseks peavad olema selged reeglid, mis hõlmavad:
   - tõrkelogide läbivaatust veendumiseks, et tõrked on rahuldavalt lahendatud;
   - parandusmeetmete läbivaatust veendumiseks, et turvameetmeid pole rikutud ja et rakendatud abinõud on täielikult volitatud.
8. Kontrolljälje tuvastatavusnõuded: allikas ja muutmise tuvastatavus ei ole olulised.
9. Kontrolljälje säilitamine: kontrolljälge tuleb säilitada vähemalt 6 kuud.

KJ-2

10. Ajalise täpsuse tagamiseks peavad süsteemide kellajad olema sünkroniseeritud
11. Kui toimiv infosüsteem ei võimalda automaatse logi pidamist, tuleb see organiseerida alternatiivsel viisil.
12. Kontrolljälje sisu: serverite/rakenduste automaatsed kontrolljäljed, mis salvestatakse kesksele logiserverile peavad sisaldama:
    - õnnestunud ja ebaõnnestunud sisse- ja väljalogimised;
    - kasutajate autentikaatorite muudatused;
    - kasutaja ID, terminali/tööjaama või juurdepääsu blokeerimine ning tegevuse põhjus;
    - pääsuõiguse keelustamist ülemääraste ebaõnnestunud sisselogimiskatsete tulemusena;
    - õnnestunud ja ebaõnnestunud info õigsuse- ja täielikkuse kontrollidest .
13. Kontrolljälje tuvastatavusnõuded: muutmine peab olema tuvastatav (seda ka juhul, kui muudatused on tehtud süsteemiülema poolt tema töö käigus).
14. Kontrolljälje analüüs: kontrolljälje analüüs peab olema graafikujärgselt korraldatud, tulemused peavad olema dokumenteeritud, kõigile juhtunud intsidentidele tuleb välja selgitada intsidendi tekke põhjus.
15. Kontrolljälje arhiveerimine: toimub logide perioodiline (kord nädalas) RO-meediale arhiveerimine, arhiivide säilitusaeg 10 aastat.

KJ-3

16. Infosüsteem (opsüsteem + rakendus) peab tagama kasutajate töö jälgimiseks kogu vajalikust/nõutavast infost kontrolljälje/logi tekkimise (vajadusel tuleb vastavad funktsioonid rakendusse/programmi lisaks programmeerida/tellida).
17. Kontrolljälje sisu: serverite/rakenduste automaatsed kontrolljäljed, mis salvestatakse kesksele logiserverile peavad sisaldama (lisaks punkt 7-le):
    - õnnestunud ja ebaõnnestunud juurdepääsud turvalisusega seotud failidele, s.h. failide loomine, avamine, sulgemine, modifitseerimine ja

kustutamine;

- priviligeeritud õigustega tehtud tegevusi süsteemi konsoolil;
- iga süsteemi juurdepääsu sessiooni algus- ja lõppaega.

18. Kontrolljälje jälgitavus: salvestatud logid peavad olema koheselt kättesaadavad selleks volitatud isikutele volitamata muutmiste viivitamatuks kontrolliks või parandamiseks, samuti muudatuste kontrollimiseks suvalisel ajal.
19. Kontrolljälje rike: kontrolljälje rikke korral peab olema tagatud protseduuriliselt alternatiivkontrolljälg (logide keskserveri HA lahendus) või süsteemi väljalülimine.
20. Kontrolljälje tuvastatavusnõuded: teabe allikas peab olema tuvastatav, logi on piisava tähtsusega, mistõttu vastutav töötleja peab saama tuvastada, kes on logi andmed sisestanud või neid viimati muutnud ja millal.
21. Automaatne kontrolljälje analüüs: kontrolljälje analüüs ja raport teostatakse automatiseeritud töövahenditega graafikujärgselt.

KJ-4

22. Pidev jälgimine: auditeerimine peab sisaldama pidevat auditeeritavate sündmuste jälgimist. Süsteem peab teavitama volitatud isikut (kasutajaabi ja monitooringu osakonda) koheselt võimalikest turvaeeskirjade rikkumistest.
23. Kontrolljälje tuvastatavusnõuded: logil peab olema tõestusväärtus, nende allikat peab saama tõestada kolmandale osapoolele - st andmed on sedavõrd kaaluka tähtsusega, et nende sisestajat või viimaste muudatuste tegijat võib olla vaja kohtus tõestada. (Seega sisuliselt kõik keskserveril salvestatavad logid peavad olema automaatselt digitaalselt allkirjastatud ning ajatembeldatud).

4.2.16. Andmete varundamine. taastamine ja saneerimine (AVT)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Andmete varundamine ja taastamine		AVT-1	AVT-2	AVT-3		AVT-1	AVT-2	AVT-3						AVT-1	AVT-2	AVT-3

Informatsiooni regulaarne varundamine on vajalik infosüsteemi töövõime taastamise tagamiseks andmete hävimise korral. Perioodiline varundatud materjalide kontroll ja taastamisvõime testimine on kinnituseks, et üldine varundusprotsess töötab.

AVT-1

1. Varundusprotseduurid: dokumenteeritud varundusprotseduurid peavad olemas olema kogu elutähtsa ja turvaga seotud informatsiooni kohta (näit. routerite tabelid, tarkvara ja dokumentatsioon).
2. Varukoopiate sagedus: varukoopiate sagedus tuleb defineerida kooskõlas andmete valdajaga ning kirjeldada varundusprotseduuris (n iga päev koopia muutustest ja kord nädalas täiskoopia vms).
3. Tsentraalse varundamise korral hoitakse kogu varundamise kohta olevat infot, kas elektroonselt või paberil (varundustellimised, -klassid, -ajakavad). Varundustellimised peavad olema allkirjastatud – kas digitaalallkiri või

tavaallkiri kui paberkujul.

AVT-2

4. Trükikoopia väljundid (paber, kile, film ja muud trükitud meediad) tuleb markeerida vastavalt akrediteeritud infosüsteemi tasemele ning soovitavalt infosüsteemi enda poolt.
5. Kõik elektroonset infot sisaldavad väljundid (magnetlindikassetid, CDd, DVDd ja muud kasutatavad meediad) tuleb markeerida.
6. Protseduuriliselt peab olema tagatud, et personal, kes käsitleb teisaldatavaid meediaid, kasutab neil nähtavaid märgistusi.
7. Varundusmeediate säilitamine: meediad, mis sisaldavad varundatud faile ja varundusdokumentatsiooni, tuleb säilitada nõutavalt spetsiaalselt kohaldatud eraldi ruumis (soovitavalt eraldi hoones), et vähendada varukoopiatel olevate andmete hävimise võimalikkust.
8. Varundusprotseduuride kontrollimine: varundusprotseduure tuleb perioodiliselt kontrollida, et tagada nende sisuline vastavus infosüsteemide kehtivate taasteplaanidega.
9. Varukoopia meedia peab olema kaitstud vähemalt ühel alljärgneval viisil:
   - peab paiknema spetsiaalselt turvatud alal (ruumis), mis tagab informatsiooni lahtise säilitamise turvalisuse;
   - ja/või peab paiknema alal, mis on pidevalt asjaomaste töötajate kontrolli all.

AVT-3

10. Varundusmeediate säilitamine: varukoopiaid, mis sisaldavad ülisalajast ja missioonikriitilist informatsiooni, tuleb säilitada vähemalt 5. km kaugusel paikneva hoone spetsiaalselt kohaldatud ruumis.
11. Informatsiooni taastamise testimine: perioodiliselt tuleb testida informatsiooni täielikku taastamist varundusmeedialt. Taastamise testimissagedus ja läbiviimine on kirjeldatud ja kehtestatud vastavas korras - see on AVT-3-le vastavatele kriitilistele (S3 ja/või K3 ja/või R3 ja/või T3) infosüsteemidele kord aastas.
12. Salajase/ülisalajase info varukoopia ja/või arhiivi meedia peab olema kaitstud:
    - andmekandjaid hoitakse selleks ettenähtud turvaseifis (st seif tulekindel, ruum veekindel) või
    - andmed krüpteeritud ja spetsiaalriistvaras (a'la RACAL, Verifone PINPad).
13. Kui salajase/ülisalajase info varukoopiat enam ei vajata, siis peab olema tagatud salajase/ülisalajase info varukoopiate ja/või selle info kandjate kindel ja ohutu saneerimine (info taastamine peab olema välistatud). Info ja/või selle kandjate hooletu kõrvaldamise tõttu võib salajane informatsioon lekkida kõrvalistele isikutele;

4.2.17. IS hooldus (ISH)

Kohustuslikud üldpõhimõtted:

- Kõigi salajase infoga tegelevate rakenduste infoedastuskanalites (klient-rakenduse server) liikuv info peab olema krüptitud - sealhulgas ka autentimis/autoriseerimisinfo.

- Ülisalajast infot (krüpteerimisvõtmed, VISA kaardivõtmed, PIN-info, …) tohib säilitada ainult krüptitult spetsiaalriistvaras või turvalises seifis (n seif tulekindel, ruum veekindel).
- Ülisalajase info kandjate füüsilistel ärastamiskatsetel peab olema tagatud andmekandja ja sellel olevate andmete füüsiline hävinemine.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS hooldus		ISH-1	ISH-2	ISH-2		ISH-1	ISH-2	ISH-2						ISH-1	ISH-2	ISH-2

Käsitluse loogilisuse ja ülevaatlikkuse huvides on infosüsteemide hooldus jagatud kaheks alamteemaks:
- üldised hooldusnõuded
- nõuded sõltuvalt töid teostavast personalist

ISH-1

Üldised hooldusnõuded:

1. Infosüsteemide valdamine: juhtkond peab looma teatava struktuuri andmete omanike ja valdajate ametlikuks määramiseks. Nende rollid ja vastutused peavad olema selgelt määratletud. Juhtkond peab tagama, et kõigile infovaradele (infosüsteemidele) on määratud valdajad, kes teevad otsuseid info turvanõuete ja pääsuõiguste kohta. Tavaliselt delegeerivad info (esma)valdajad infosüsteemi(de) hoolduse IT ekspluatatsioonirühmale, turvakohustused aga andmeturbejuhile. Asjakohaste turvameetmete käigushoiu eest jäävad aga infovarade omaniku ees esmavastutavaiks esmavaldajad. (Peadirektori käskkiri, et andmete valdajaks on põhitegevusvaldkond ja infotöötlusvahendite valdajaks IT osakond.)
2. Peab olema tagatud, et muudatuste teostamine leiab aset sobival ajal ega häiri äriprotsesse, mida konkreetne muudatus puudutab.
3. Muudatuste juhtimine tavaolukorras: turvameetmete muudatuste üle peab otsustama IT juht.
4. Muudatuste juhtimine kriisiolukordades: andmeturbe eest vastutava isiku ülesandeks on korraldada kõigi väljaspool tavapärast muudatuste juhtimist olevate muudatuste (kiirmuudatused) teostamine ning samas tagades, et need muudatused oleksid nii tehniliselt kui protseduuriliselt lubatavad.
5. Infosüsteemide rikkumise vältimiseks peab muudatuste teostamine olema range kontrolli all, eelnevalt testitud ja dokumenteeritud ning kõik muudatused tuleb logida.
6. Muudatusi tohib teha vaid selleks volitatud personal.
7. Muudatused, mis mõjutavad süsteemi turvet, kinnitab IS-de ekspluatatsiooni/hoolduse eest vastutav isik.
8. Infosüsteemide ekspluatatsiooni/hoolduse eest vastutav isik peab määrama hoolduspäeviku (mis teha) ning hoolduslogi (mis tehtud) vajaduse ja formaadi.
9. Andmesisestust rakendussüsteemidesse tuleb valideerida veendumiseks, et info on õige ja täielik.

10. Hoolduspäevik ja hooldusLogid peavad sisaldama jälje info õigsuse ja täielikkuse nõutavate kontrollide teostamisest ning nende õnnestumistest ja ebaõnnestumistest.

11. Süsteemi hooldustööd tuleb läbi viia võimaluse korral asutuse ruumides. Seadmed, mida remonditakse väljaspool ja mis peavad olema turvatud, tuleb turvalisuse tagamisnõue fikseerida vastavas lepingus.

12. Kui süsteemid või selle komponendid on väljastatud remonti, tuleb need eelnevalt saneerida kõigist salajastest või tundlikest andmetest kooskõlas andmeturbejuhi poolt kinnitatud protseduuridele . Kõikide süsteemide ja nende osade väljasaatmise kinnitab IT ekspluatatsiooni/hoolduse eest vastutav isik.

13. Võrguanalüsaatorid (nt sniffer) peavad olema kinnitatud andmeturbejuhi poolt enne nende rakendamist süsteemis. Andmeturbejuht peab kinnitama selliste seadmete kasutamise asutusevälise hooldusPersonali korral, kui süsteemi ei ole võimalik saneerida salajasest või tundlikust informatsioonist. IT juht peab kinnitama selliste seadmete kasutamise hooldusPersonali korral, kellel on juurdepääs kõrgeima tundlikkusastmega informatsioonile süsteemis.

14. Tarkvara väljatöötajate poolt loodud vaikimisi kasutajad ja nende paroolid peab asendama koheselt pärast tarkvara installeerimist.

15. Peab olema tagatud, et enne kasutamist infotöötlusressursid ei sisalda jääkandmeid.

16. Kui hooldusPersonal toob asutusse kaasa diagnostika- ja/või testprogramme, tuleb:
    - enne kasutamist kontrollida meediat, mis sisaldab testprogramme, et see ei sisaldaks ründeprogramme.
    - meediaga, mida korduvalt kasutatakse, peab jääma asutuse turvatsooni ning tuleb arhiveerida vastavalt diagnoositava infosüsteemi turvatasemele.
    - enne asutusse sisenemist tuleb hooldusPersonali informeerida sellest, et neil ei ole lubatud, ilma spetsiaalset kontrolli läbimata, meediat asutusest välja viia.
    - Kui eelnevat ei ole võimalik rakendada eritingimuste tõttu, peab meedia läbima tugevdatud tervikluse kontrolli (näit. viirusekontroll, kontrollsummad, vms.) enne selle kasutamist infosüsteemis ning enne asutusest lahkumist tuleb meedia üle kontrollida, et salajasi andmeid ei oleks meediale kirjutatud. Ülevaatusprotseduuri peab asutuse andmeturbe eest vastutav isik.

17. Kõiki diagnostikaseadmeid ja muid hooldusPersonali poolt asutusse toodavaid seadmeid tuleb käsitleda alljärgnevalt:
    - Asutuse ruumidesse toodavaid süsteeme ja süsteemi komponente tuleb pisteliselt kontrollida, et need ei mõju kahjulikult infosüsteemi turvalisusele.
    - Enne seadmete väljaviimist tuleb hooldusseadmed, mis võimaldavad salvestada informatsiooni, saneerida andmeturbe eest vastutava isiku poolt kehtestatud protseduuri järgi. Kui seadmeid ei saa saneerida, siis need kas peavad jääma asutuse ruumidesse, hävitatakse või väljastatakse andmeturbejuhi poolt kinnitatud protseduuri alusel.
    - Asendatavaid komponente võib tuua asutuse ruumidesse ainult vastavates seadmetes vahetamiseks, tagatud peab olema kontroll varukomponentide säilitamisel ja kasutuselevõtmisel. Kõik eelnevalt

infosüsteemis olnud komponendid tuleb kuni väljastusprotseduuride täitmiseni jätta asutuse ruumidesse. Kõik komponendid, mis ei olnud eelnevalt infosüsteemis, võib väljastada kui vahetus toimus kvalifitseeritud/volitatud asutuse IT personali juuresolekul või on üle vaadatud vastavalt nõutavatele väljastusprotseduuridele.

18. Peale hooldust tuleb üle kontrollida süsteemi turvarakendused, et tagada nende korrektne töö. Tulemused dokumenteerida.

19. Tuleb evitada asjakohased protseduurid vastavuse tagamiseks õiguslikele kitsendustele materjali kasutamisel, mille suhtes võivad kehtida intellektuaalse omandi õigused (näiteks autoriõigus või kaubamärgiõigus);

20. Peab olema tagatud, et konfidentsiaalset informatsiooni käsitleval raportil/dokumendil on selgesõnaliselt ja arusaadavalt igal lehel kirjutatud raporti salajasuse aste (sisemiseks kasutuseks, salajane, ülisalajane), nii et on tagatud märgendite viivitamatu mõistmine ja informatsiooni asjakohane kaitse. Vastavasisuline märgend peab olema kättesaadav vaid selleks volitatud inimestele.

21. Kui infokandjaid enam ei vajata, tuleb nad turvaliselt ja ohutult kõrvaldada. Infokandjate hooletu kõrvaldamise tõttu võib salajane informatsioon lekkida kõrvalistele isikutele. Riski minimeerimiseks tuleb kehtestada formaalsed protseduurid infokandjate turvaliseks kõrvaldamiseks. Vaid volitatud personal võib tegeleda infokandjate kõrvaldamisega.

Nõuded hooldusele sõltuvalt töid teostavast personalist

Asutusesisene hoolduspersonal:

22. Personal, kes viib läbi süsteemihooldust, peab omama selleks volitust. Hooldustööde teostamisel tuleb järgida tootjapoolseid juhiseid ning kehtivaid turva- ja tööohutuseeskirju.

23. Infosüsteemide haldusutiliitide kasutamine peab olema range kontrolli all.

Asutuseväline hoolduspersonal:

24. Kui on vajadus asutuseväliste hooldusisikute kaasamiseks hooldustöödes, siis tuleb neid isikuid jälgida kvalifitseeritud/volitatud asutuse IT personalil ning kirjeldada nende tegevused hoolduspäevikusse.

25. Hooldustöödes kaasatavate Asutuseväliste kolmandate osapoolte spetsialistidega tuleb sõlmida töö käigus saadud konfidentsiaalse informatsiooni mitteavalikustamise kokkulepped.

26. Kolmandate osapoolte töötajatele ei tohi anda juurdepääsu informatsioonile ega infotöötlusvahenditele enne kui on evitatud asjakohased turvameetmed ja alla kirjutatud leping, mis määratleb ühenduse või juurdepääsu tingimused.

27. Enne hooldustöid on soovitav süsteem täielikult saneerida ning teisaldatavad andmekandjad eemaldada või välja lülitada. Kui süsteemi ei saa saneerida tuleb kasutada Andmeturbejuhi poolt kinnitatud protseduure, mis peavad välistama asutuseväliste hooldusisikute visuaalse või elektroonilise juurdepääsu süsteemi salajastele või tundlikele andmetele.

28. Asutusevälise hoolduspersonali poolt läbiviidavate hooldustööde jaoks peab olema eraldi koopia haldusutiliitidest ja operatsioonisüsteemist kaasa arvatud disketid, lindikassetid või CD-d. Koopial peab olema nähtaval märgistus "AINULT HOOLDUSTÖÖDEKS" ning see peab olema kaitstud vastavalt

dokumenteeritud protseduuridele. Infosüsteemide hooldusprotseduurid, kus kasutatakse mitteteisaldataval salvestusseadmel (kõvakettal) paiknevat operatsioonisüsteemi, tuleb realiseerida igal konkreetsel juhul eraldi.

29. Asutusevälisele hoolduspersonalile kuuluvad ja asutuse andmesidevõrku ühendamist võimaldavad edastusvõimega andmesideseadmed ning ükskõik milline andmete salvestusmeedia, mis ei ole seotud hooldusvisiidiga või tarne-/hoolduslepinguga, peavad jääma väljapoole süsteemi ruume ja tagastatakse hoolduspersonalile nende lahkumisel asutusest.

Kaughooldus:

30. Kaughooldust võib rakendada vastavalt lepingutele kolmandate osapooltega ning ainult juhul kui teenuse pakkuja turvalisuse tagamise kriteeriumid on samaväärsed asutuse omadega.
31. Infosüsteem peab olema saneeritud ja eraldatud teistest süsteemidest enne kaugjuurdepääsuga ühendamist.
32. Kui süsteemi ei ole võimalik saneerida salajastest või tundlikest andmetest (nt süsteemi avarii korral), siis kaugdiagnostika ja hooldustööd ei ole lubatud.
33. IS hoolduse eest vastutav isik peab korraldama kaugjuurdepääsu lubamise ja lõpetamise.
34. Tegevustest peab säilima kontrolljälg. Hooldustööde läbiviijaid tuleb sellest enne tööde teostamist teavitada.
35. Tehniliselt kvalifitseeritud isik peab teostama hoolduslogi revisjoni võimalike volitamata muudatuste väljaselgitamiseks.
36. Hoolduspersonal kellel on juurdepääs infosüsteemile kaughooldepunktist peab omama tööde teostamiseks volitust ning olema sõlmitud konfidentsiaalsusleping (usaldusleping).
37. Protseduurid kaugdiagnostika ühenduste installeerimiseks peavad olema kinnitatud andmeturbejuhi poolt.
38. Kõikide kaughoolduse ja diagnostika teenuste kohta peab olema kontrolljälg.

ISH-2

39. Kõikide kaughoolduse ja diagnostika teenuste logid tuleb salvestada spetsiaalsele eraldiasuvale logiserverile
40. Kõikide info õigsuse ja täielikkuse kontrollide logid tuleb salvestada spetsiaalsele eraldiasuvale logiserverile
41. Nõutav diagnostikaühenduste krüpteerimine, tugevate autentimis-tehnoloogiate (nt *token device*) kasutamine ja kaugühenduse katkestamise kinnitamine.

4.2.18. Infoturvaintsidentide haldus (TIH)

Turvaintsidentide haldus on üldjuhul IS hoolduse tegevusvaldkond, kuid see on väga oluline infoturbe tegevusvaldkond ning selle pärast on eraldi teemana välja toodud.

TIH-1

1. Kõikidest probleemidest/turvaintsidentidest ja hädaolukordadest on asutuse töötajad kohustatud informeerima kasutajaabi ja IT valvepersonali, kes kontrollib häire adekvaatsust ja vea ulatust, organiseerib edasise informeerimise ja vajaliku abi.

2. Turvaintsidendi korral peab toimuma kiire ja tõrgeteta reageerimine ning vajadusel koostöö korrakaitseorganite, ametiasutuste, infoteenuste andjate ja sideoperaatoritega;
3. Intsidendile kiireks reageerimiseks peavad ja võivad ainult volitatud isikud suhelda korrakaitseorganite, ametiasutuste, infoteenuste andjate ja sideoperaatoritega.
4. IT valdkonna töötaja on turvaintsidendi, hädaolukorra või globaalse hädaolukorra tuvastamise järel samuti kohustatud koheselt informeerima kasutajaabi ja IT valvepersonali ning seejärel aitama kaasa vea olemasolu kontrollimise ja ulatuse määramise osas volituste, võimaluse ja oskuste olemasolul asuma viga likvideerima.
5. Turvaintsidendi tuvastamise või sellekohase signaali saamise järel vastutavad kasutajaabi või IT valvepersonal edasise vajaliku info liikumise eest. Selleks ta:
   - registreerib intsidendi häiresignaali ning kontrollib vea tõesust ning ulatust;
   - määratleda turvaintsidentide raporteeritavad sümptomid ning fikseerida kõik ekraanile ilmuvad teated;
   - informeerib IT vastutavas valves olevat isikut;
   - informeerib asjasse puutuva IT valdkonna juhti;
6. Juhul kui tegemist on hädaolukorraga (st turvaintsident on ajaliselt kestnud üle turvanõuetega määratletud lubatava aja):
   - informeerib IT hooldusjuhti ning vajadusel IT juhti või muid isikuid.
   - vajadusel informeeritakse põhitegevusvaldkonna esindajaid ning toimub see IT valdkonna juhtide tasemel.
7. Infoturbe intsidendi haldus peab, peale intsidendi tuvastamist ja vajalike persoonide kohest informeerimist, pidevalt jälgima ja vahendama informatsiooni intsidendi lahendamiskäigust kuni selle lahendamise/likvideerimiseni.
8. Vea likvideerimise järel on IT valdkonna töötaja kohustatud informeerima abiliini, IT valvepersonali ja enda otsest juhti.
9. Ajakirjandusega suhtlemine toimub ainult läbi pressibüroo või IT juhi.
10. Kasutajad ei tohi püüda kõrvaldada kahtlustatavat tarkvara, kui nad ei ole volitatud seda tegema.
11. Kasutajatelt saadud tõrketeated infotöötlus- või sidesüsteemide probleemide kohta tuleb logida.
12. Tõrgete käsitluseks peavad olema selged reeglid, mis hõlmavad tõrkelogide läbivaatust veendumaks, et turvameetmeid pole rikutud ja tõrked on rahuldavalt lahendatud.

TIH-2

13. Sunnihäire(te)le reageerimiseks (kui see on riskide hindamisel vajalikuks peetud) peavad olema määratletud kohustused ja kehtestatud protseduurid.
14. Hädaolukorra (näit. mingi olulise süsteemi peatumine/hangumine) tuvastamisel informeerib kasutajaabi IT hooldusjuhti või teda asendavat isikut, kes kutsub vea tehniliste põhjuste väljaselgitamiseks kokku IT asjasse puutuvate struktuuriüksuste juhid ja spetsialistid, kes arutavad läbi edasise tegevusplaani. Olukorrast üldpildi saamise järel peab IT hooldusjuht koheselt (töövälisel ajal

juhtunud intsidendist vähemalt järgmise tööpäeva alguses) teavitama IT juhti. Üldjuhul käitutakse vastavalt infosüsteemi(de) taasteplaani(de)le.

15. IT juht annab põhitegevusvaldkondadele informatsiooni hädaolukorra, võimaliku IT süsteemide seisaku ja selle kestvuse ning muude asjaolude kohta. Lisaks teavitab IT juht vajadusel oma otsest ülemust ning pressibüroo töötajat.
16. Globaalse hädaolukorra korral (näit. asutuse serveriruum ja selles oleva arvutustehnika, enamuse oluliste süsteemide peatumine/hävimine vms), kui kogu asutuse töö on häiritud või peatunud, teavitab monitoorija sellest asutuse IT juhti ja asutuse IT kõiki struktuuriüksuste juhte, asutuse Kriisijuhti, asutuse asjasse puutuvate osakondade ja büroode juhte. Üldjuhul käitutakse vastavalt talitluspidevus- ja taasteplaanile.
17. Hädaolukorra lahenemise järel toimub sellest teatamine sarnaselt häireolukorrast teatamisele, st. monitoorija on kohustatud informeerima sellest kõiki isikuid, kellele ta teatas häirest.

4.2.19. IS arendus (ISA)

Peab olema tagatud, et turvalised on nii infosüsteemide arendus kui protsess ise kui ka arenduse tulemusena tekkiv uus infosüsteem tulevases ekspluatatsioonis.

NB! Infosüsteemide/rakenduste sisseostmine on samuti arendus.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS arendus		ISA-1	ISA-2	ISA-2		ISA-1	ISA-2	ISA-2						ISA-1	ISA-2	ISA-2

ISA-1

1. Arenduskeskkond ise on infosüsteem, millele määratakse vajalikud turvameetmed vastavalt korrale.
2. IS arendusel ja arenduste testimisel tuleb arvestada infosüsteemile tulevases ekspluatatsioonis esitatavaid turvanõudeid, mille tagamiseks vajalikud turvameetmed (vastavalt käesolevale korrale) peavad olema realiseeritud/testitud - eriti olulist tähelepanu vajavad sellised teemad nagu
   - autentimine/autoriseerimine,
   - krüpteerimine,
   - kasutajate töö jälgitavus,
   - rakenduse töös ilmneda võivate turvaintsidentide monitooritavus,
   - info õigsuse ja täielikkuse nõutav perioodiline või reaalajas kontrollimine,
   - kontrolljälje tekitamine õnnestunud ja ebaõnnestunud info õigsuse- ja täielikkuse kontrollidest .
3. Projekteeritavate turvameetmete majandusliku otstarbekuse tagamiseks peab kasutama infovarade väärtusele vastavaid turvameetmeid. Et hinnata rakendatavate meetmete otstarbekust tuleb määrata turvameetmete rahaline väärtus. Turvameetmed on oluliselt odavamad ja tõhusamad kui nad kavandatakse rakendussüsteemidesse nõuete spetsifitseerimise ja projekteerimise faasis.
4. Programmide rikkumise võimaluse vähendamiseks tuleb rangelt reguleerida juurdepääsu programmide lähtekoodide teekidele. Tuleb vältida lähtekoodi teekide hoidmist tootmissüsteemides. Programmide lähtekoodi vanad

versioonid tuleb arhiveerida, märkides selgelt nende kasutuseloleku kuupäevad ja kellaajad, koos kogu tugitarkvaraga, tootejuhtimisega, andmemääratlustega ja protseduuridega.

5. Ettevõtte IS arendusmeeskond peab kasutama turvalisi programmeerimismetoodikaid ning tagama sellega ettevõtte siseselt arendatavate koodide turvalisuse.
6. Arenduse käigus peab olema tagatud, et salajase informatsiooni käsitlemisel selgesõnaliselt ja arusaadavalt igale lehele kirjutatakse raporti salajasuse aste (sisemiseks kasutuseks, salajane, ülisalajane), nii et on tagatud märgendite viivitamatu mõistmine ja informatsiooni asjakohane kaitse. Märgend peab olema nii väljatrükitud kui ka elektroonsel kujul oleva konfidentsiaalse dokumendi igal lehel.
7. Sisseostetud tarkvarapakettide modifitseerimisest tuleb hoiduda. Võimaluse korral tuleb tarnitud tarkvarapakette kasutada muudatusteta. Vältimatu muutmise vajadusel tuleb hankida tarnija nõusolek. Kui vähegi on võimalik tuleb nõutavad muudatused saada tarnijalt tavaliste programmivärskendustena. Kui muudatusi loetakse olulisteks, tuleb algne tarkvara säilitada ning muudatused teha selgelt märgistatud koopias.

ISA- 2

8. Arendamisel ei tohi eriloata kasutada reaalset infot.
9. Arendus(t)e ja käikuantud süsteemide haldus peab olema eraldatud.
10. Vajaduse korral tuleb infosüsteemis luua sunnialarmi võimalus. Otsus sellise alarmi vajalikkuse kohta peab põhinema riskide hindamisel.
11. mõned rakendussüsteemid on võimalikele kadudele küllaltki tundlikud ja nõuavad erikäsitlust. Tundlikkus võib viidata sellele, et rakendussüsteemi tuleb käitada eriti turvaliseks tunnistatud arvutil/operatsioonisüsteemil, et ta peab ressursse ühiselt kasutama ainult koos usaldusväärsete rakendussüsteemidega või et tal ei tohi olla kitsendusi.
12. Programme tuleb võimaluse korral osta lähtekoodi kujul mainekast (tuntud) firmast, nii et koodi saab verifitseerida. Võimaluste piires kontrollida kogu kood enne kasutamist;
13. Väljast tellitavatele tarkvaraarendusprojektide lepingutele lisada koodi omandiõigus, intellektuaalne omandiõigus ja litsentsilepingud, nõuda installeerimiseelset testimist õelkoodi jms avastamiseks, töö kvaliteedi ja õigsuse tõendamist;

4.2.20. Infosüsteemi testimine (IST)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS testimine		IST-1	IST-2	IST-2		IST-1	IST-2	IST-2						IST-1	IST-2	IST-2

Infosüsteemide testimine on tegevus, mille eesmärgiks on defektide avastamine või nende puudumise hindamine testitavas infosüsteemis. Infoturbes kasutatakse testimist turvaprotsesside ja turvameetmete kvaliteedi tagamiseks. Oluline on, et IS testides on vajalik ka IS turvalisuse testimine.

IST-1

Infosüsteemide ja nende turvalisuse testimise nõuded:

1. Testimise algatab infosüsteemi valdaja või andmeturbejuht.
2. Testimise läbiviimiseks tuleb määratleda järgmised parameetrid:
   - mida testida - testobjekt (riistvara, tarkvara, andmed)
   - kus testida - testkeskkond (arendus- või tootmissüsteem, sertifitseeritud, ühilduv, sarnane)
   - millega testida - testandmed (põhitegevussüsteemi andmed, modifitseeritud põhitegevussüsteemi andmed, testimiseks spetsiaalselt genereeritud andmed)
   - kes testivad - läbiviijad (arendajad, sõltumatud testijad)
   - kuidas testida - alginfo testobjekti kohta (must kast, valge kast)
   - kui palju testida - testide kate
   - kui "täpselt" testida - hindamiskriteeriumid (korras/viga, korras/ohtlik/.../viga)
3. Testimist tohib läbiviia ainult kooskõlastatult testitava infosüsteemi (potentsiaalse) valdajaga, kes kinnitab testimise parameetrid.
4. Testimisel tuleb järgida testitava infosüsteemi turvanõudeid. Vajadusel rakendatakse meetmeid turvanõuete tagamiseks (eraldatud keskkonnad, genereeritud testandmed vms).
5. Testimisel tuleb arvestada testimisprotsessi läbiviimise ja testimistulemustega seonduvaid ohte (nt. testimisaruande lekkimine).
6. Testimisprotsessi läbiviimine, testimisobjekti, –keskkonna, –andmete ja –dokumentatsiooni käsitlemine peavad olema kirjeldatud vastava korraga.
7. Testimisprotsessi läbiviimisel tuleb vältida huvide konflikte (nt. süsteemi väljatöötajad ei tohi olla testide väljatöötajateks).
8. Testimine peab olema majanduslikult efektiivne (tehtavad kulutused peavad olema vastavuses saadava tuluga).
9. Kõik muudatused tuleb täielikult testida ja dokumenteerida, nii et neid saab vajaduse korral uuesti rakendada tarkvara tulevastes värskendustes.

IST- 2

10. Testimisel ei tohi eriloata kasutada reaalset infot.
11. Testima peab info õigsuse ja täielikkuse piisavate kontrollide olemasolu ja õigsust ning vastavatest tegevustest kontrolljälje tekkimist.
12. Testimine peab aset leidma infosüsteemi väljatöötamisel/modifitseerimisel enne (taas)kasutamist ja akrediteerimist.
13. Testimist tohib läbiviia ainult kooskõlastatult andmeturbejuhiga, kes kinnitab testimise parameetrid.

4.2.21. Ajakohastamine, kontroll ja turvatestimine (AKT)

Ajakohastamine:

- Peab olema süsteem, et jälgida väljatulekut ja siis ka teostada opsüsteemide, baastarkvara ja rakenduste täiendused (*upgrade*'id), hädaparandused (*patch*'id) ja turvaparandused (*security patch*'id)
- Peab olema spetsiaaltarkvara, et kontrollida perioodiliselt opsüsteemide, olulise baastarkvara (n faili-, meili-, andmebaasi-, veebi- jms serverid) ja rakenduste patch'ide/upgrade'ide teostatust

Kontroll:

Peab olema spetsiaaltarkvara, et kontrollida perioodiliselt (et mingi upgrade, patch, installatsioon pole mingit olulist setingut muutnud):

- oluliste süsteemsete (opsüsteemide, andmebaaside, veebiserverite jms) failide kaitstust
- rakenduste oluliste/salajaste failide kaitstust
- andmebaaside kui failide kaitstus
- pääsusüsteemi (access control system) oluliste (kasutajad, paroolid, võtmed) failide kaitstus
- paroolimurdmiskatsete tuvastamine

Turvatestid:

- paroolide piisava keerukuse testimine paroolimurdjaga
- sissemurdmistest (Penetration Test)
- rakenduste turvalisuse testid

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Infoturbe ajakohastamine, kontroll ja testimine		AKT-1	AKT-2	AKT-3										AKT-1	AKT-2	AKT-3

AKT-1

1. Peab olema süsteem, et jälgida paranduste väljatulekut ja siis ka teostada opsüsteemide, baastarkvara ja rakenduste täiendused (*upgrade*'id), hädaparandused (*patch*'id) ja turvaparandused (*security patch*'id)
2. Kõik täienduste ja paranduste teostamised peavad olema dokumenteeritud.

AKT- 2

3. Peab olema spetsiaaltarkvara, et kontrollida perioodiliselt opsüsteemide, olulise baastarkvara (n faili-, meili-, andmebaasi-, veebi- jms serverid) ja rakenduste patch'ide/upgrade'ide teostatust
4. Peab olema spetsiaaltarkvara, et kontrollida perioodiliselt (et mingi upgrade, patch, installatsioon pole mingit olulist setingut muutnud):
    - oluliste süsteemsete (opsüsteemide, andmebaaside, veebiserverite jms) failide kaitstust
    - rakenduste oluliste/salajaste failide kaitstust
    - andmebaaside kui failide kaitstus
    - pääsusüsteemi (access control system) oluliste (kasutajad, paroolid, võtmed) failide kaitstus
    - paroolimurdmiskatsete tuvastamine
5. Perioodiliselt peab tegema järgnevaid turvateste:
    - paroolide piisava keerukuse testimine paroolimurdjaga – kord kuus

AKT- 3

6. Perioodiliselt peab tegema järgnevaid turvateste:
    - sissemurdmistest (Penetration Test) – kord aastas
    - missioonikriitiliste rakenduste turvalisust peab testima kord aastas

TALITLUSPIDEVUS

4.2.22. Talitluspidevuse- ja taasteplaanid (TPT)

Asutuse talitluspidevuse strateegiaks on talitluspidevuse plaani välja töötamine, juurutamine ning selle alahoid kõigi põhitegevusprotsesside osas, mis toetavad olulisi asutuseteenuseid kriisiolukordades. Kriisiolukorras osutatavate asutuse teenuste hulk on kindlaks määratud asutuse põhiprotsesside analüüsiga.
Talitluspidevuse plaanimine peab hõlmama meetmeid riskide tuvastamiseks ja leevendamiseks, leevendama õnnetuse võimalikke tagajärgi ning tagama elutähtsate toimingute kiire jätkamise.
Talitluspidevuse plaanid peavad hõlmama: isikuid, kes vastutavad põhitegevusprotsesside läbiviimise eest, vajalikke ruume, IT-d, telekommunikatsioone, infrastruktuuriteenuseid ja juhendmaterjale. Vajalikud on ka põhitegevusprotsesside taasteplaanid nendele olukordadele, kus ei ole võimalik kasutada tavapärast töökeskkonda ning -protseduure.
Talitluspidevusplaanile ülemineku korralduse peab andma asutuse kriisijuht, sest talitluspidevust tagavatest käsitsitöö ja/või autonoomsetest protsessidest normaalsesse tegevusse tagasiminek on üldjuhul vägagi töömahukas.

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
Talitluspidevuse- ja taasteplaanid						TPT-1	TPT-2	TPT-3		TPT-1	TPT-2	TPT-3				

TPT- 1

1. Plaani otsustus: süsteemi valdaja peab välja selgitama talitluspidevuse vajalikkuse:
    - talitluspidevuse plaani mittevajalikkusest peab olema ka sellekohane kirjalik otsus.
    - kui aegkriitilisuse ja tagajärgede kaalukusega K1/R1 infosüsteemile leitakse talitluspidevuse plaan (erijuhul) oluline ja vajalik olevat, siis jätkatakse vastavalt TPT-2'le.

TPT- 2

2. Plaani koostamine: tuleb koostada talitluspidevuse plaanid infosüsteemidele, milliste kohta on tehtud otsus selle vajalikkusest.
3. Äritegevuse jätkuvuse tagamise planeerimine peab algama äriprotsesside katkemist põhjustada võivate sündmuste väljaselgitamisest. Tähelepanu tuleb pöörata väliste ärisõltuvuste hindamisele ja sõlmitud lepingutele;
4. Talitluspidevuse plaanil peab olema juhtkonna poolne toetus ja vastavasisuline kinnitus.
5. Talitluspidevuse protseduurid (peavad olema kirjeldatud talitluspidevuse plaanis):
    - *Eriolukorrad (sõjaseisukord, rahutused, suured looduskatastroofid jms)* – kirjeldatud käitumist ja nõudeid/eesmärke eriolukordades, st arvestades

raskendavaid asjaolusid on loogilised piiratud (ainult kõige olulisemad) funktsionaalsus, madalamad nõuded käideldavusele ja terviklusele, ajutised laiendatud volitused teatud otsuste tegemiseks;
- *erakorralised protseduurid (intsidentide käsitlemine)* — kirjeldavad vahetuid toiminguid pärast talitlusoperatsioone ja/või inimelusid ohustavat õnnetust;
- *taandeprotseduurid* — kirjeldavad vajalikke toiminguid, mis tuleb sooritada oluliste talitlusoperatsioonide üleviimiseks alternatiivsesse ajutisse asukohta;
- *taasteprotseduurid* — kirjeldavad toiminguid, mis tuleb sooritada normaalsete talitlusoperatsioonide taastamiseks (tavaliselt esialgses asukohas);
- *testi kirjeldus* — kuidas plaani testitakse;
- *alalhoid/hooldamine* — plaani igal tasemel ning igal üksikplaanil peab olema omaette hooldaja, kes vastutab plaani ajakohasuse eest;
- *koolitus* — töötajaskond peab mõistma talitluspidevuse eesmärki ning olema koolitatud oma rolli läbiviimiseks talitluspidevuse protsessis;
- talitluspidevusplaanidele peab lisama või selles viitama vajalikele varundus- ja taastetegevustega seotud protseduuridele.

6. Protseduuride kaasajastamine: protseduure tuleb perioodiliselt kaasajastada, et tagada viimase versiooni vastavus protseduurijuhistele. Kaasajastamise sageduse määrab andmeturbejuht kooskõlas infosüsteemi valdaja(te)ga.
7. Selgitus: töötajaskond peab mõistma talitluspidevuse eesmärki ning olema teadlik oma rollist konkreetses talitluspidevuse protsessis.

TPT- 3

8. Talitluspidevusplaani testimine: protseduure tuleb perioodiliselt kaasajastada ja testida, et tagada viimase versiooni vastavus protseduurijuhistele. Talitluspidevusplaani testimiseks tuleb koostada testplaan koos testide läbiviimise graafikuga ja testimistulemuste hindamisega. Testimise sageduse määrab andmeturbejuht kooskõlas infosüsteemi valdaja(te)ga.
9. Koolitus: töötajaskond peab olema koolitatud oma rolli läbiviimiseks talitluspidevuse protsessis. Koolitamise sageduse määrab andmeturbejuht kooskõlas infosüsteemi valdaja(te)ga.
10. Erinõuded missioonikriitiliste 7x24 infosüsteemide talitluspidevuse ja taasteplaanide koostamisele: talitluspidevuse plaane tuleb kord aastas ajakohastada, töötajaskond koolitada ning kogu talitluspidevuse- ja taasteplaanid reaalselt ja täies mahus testida.

4.2.23. Infosüsteemide taasteplaanid (ISTP)

	S0	S1	S2	S3	K0	K1	K2	K3	R0	R1	R2	R3	T0	T1	T2	T3
IS taasteplaanid		ISTP-1	ISTP-2	ISTP-3		ISTP-1	ISTP-2	ISTP-3		ISTP-1	ISTP-2	ISTP-3		ISTP-1	ISTP-2	ISTP-3

Infosüsteemi taastamise all tuleb mõista funktsioone, mida tuleb täita IS-i rikke või talitluse katkemisel. Taastetegevused peavad kindlustama, et turvaintsidendi järel IS saavutab nõutava/aktsepteeritava (käideldavuse nõuetest aegkriitilisus) ajaga taseme, kus süsteemi kõik funktsioonid (kindlasti ka turvafunktsioonid) on

taastatud.

ISTP-1

1. Taasteprotseduurideks vajaliku info kättesaadavus: infosüsteemi tehniline info (süsteemi ja rakenduse administraatorite kontaktinfo, paroolid, koodid, süsteemide käsiraamatud) ja taasteprotseduure kirjeldav dokumentatsioon peab olema ajakohane ja kättesaadav.
2. Taaste järelvalve: peavad eksisteerima dokumenteeritud protseduurid ja süsteemsed võimalused, et kindlustada infosüsteemide taastamise kontroll. Tavaolukorrast kõrvalekallete ilmnemisel tuleb probleemide lahendamiseks kontakteeruda IT hooldusjuhi või andmeturbejuhiga.
3. Koostöö lepingupartneritega: turvaintsidendist informeerimisel, kaugdiagnostika läbiviimisel jms on eriti oluline sõlmitud lepingute täpne järgimine.

ISTP-2

4. Taaste usalduslikkus: peavad olema rakendatud protseduurid ja tagatud tehniliste süsteemide võimalused süsteemi taastamise usaldatavuse ja turvalisuse kindlustamiseks.
5. Tegevused, mille tulemus ei taga süsteemi kaitsetingimuste täielikku taastamist, peavad olema dokumenteeritud.
8. Protseduuride kaasajastamine ja testimine: protseduure tuleb perioodiliselt kaasajastada ja testida, et tagada viimase versiooni vastavus protseduurijuhistele. Kaasajastamise ja testimise sageduse määrab IT hooldusjuht kooskõlas infosüsteemi valdaja(te)ga.
9. Dubleerimine: peab olema tagatud analoogse infotöötluskeskkonna tekitamine käideldavusnõuetega (aegkriitilisus) määratletud aja jooksul.
10. Talitluspidevusplaanile üleminek: kui on selgunud süsteemi taaste võimatus käideldavusnõuetega (aegkriitilisus) määratletud aja jooksul, tuleb kaaluda üleminekut talitluspidevusplaaniga määratud tegutsemisreeglitele. Talitluspidevusplaanile ülemineku korralduse peab andma asutuse kriisijuht, sest talitluspidevuse käsitsitöö ja/või autonoomsetest protsessidest normaalsesse tegevusse tagasiminek on üldjuhul väga töömahukas.

ISTP-3

11. Taasteplaani testimine: taasteplaani testimiseks tuleb koostada testplaan koos testide läbiviimise graafikuga ja testimistulemuste hindamisega.
12. Täielik infotöötlusressursi dubleerimine: rikke puhul toimub ümberlülimine identsele varuinfotöötlusressursile.
13. Erinõuded missioonikriitiliste 7x24 infosüsteemide taasteplaanidele: taasteplaane tuleb kord aastas ajakohastada, töötajaskond koolitada ning taasteplaanid reaalselt ja täies mahus testida.