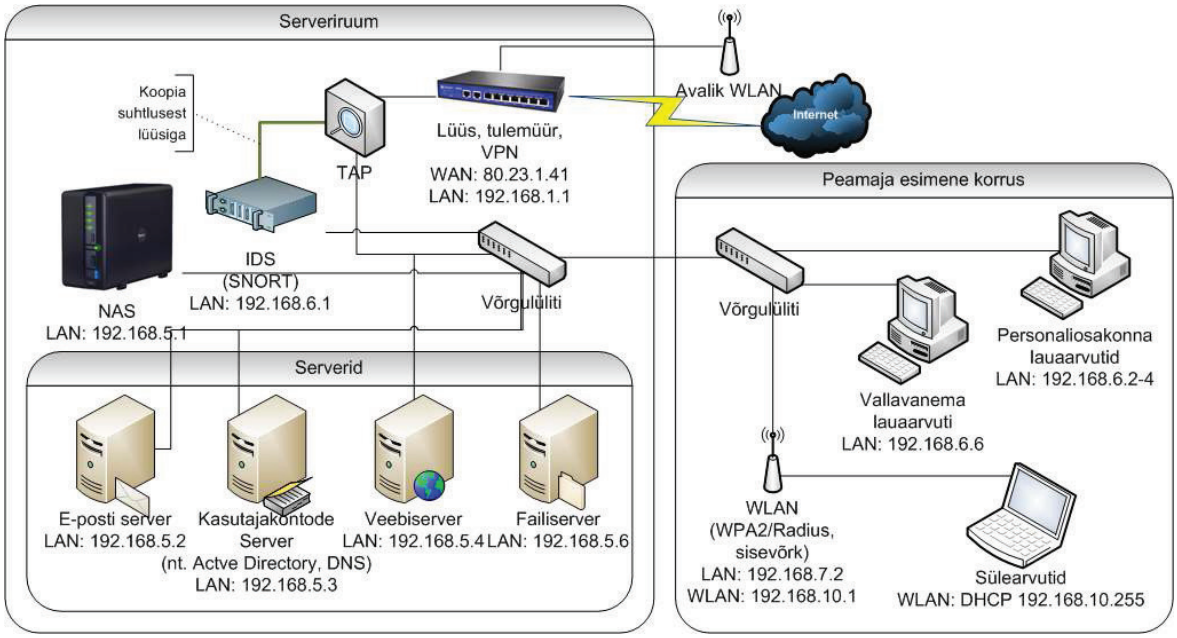
6 SEADISTUSJUHENDID

Seadistusjuhendites on välja toodud mõned olulisemate süsteemi komponentide seadistused. Alates ISKE 5.00 versioonist on enamus meetmeid saanud täistõlke, seetõttu ei pea me otstarbekaks neid siinkohal veel eraldi refereerida. Lähtume pigem olulisemate seadistusjuhiste komplektide väljatoomisest ja seostega arvestamisest, täpsemad juhised annab aga ISKE meetmete kataloog.

6.1 VÕRGUSKEEMI NÄIDIS

Võrguskeemile tuleks seadmete kohta märkida:

- Seadmete identifikaatorid
- Seadmete nimed
- Võrguühenduste aadressid (IPv4, IPv6, IPX ning soovi korral MAC) või nende vahemikud
- Soovi korral muu info (nt seadmete rollid, operatsioonisüsteem, jms), mis tööd lihtsustab
- Võrguskeemil on mõistlik ühes võrgu piirkonnas asuvad üheotstarbelised seadmed grupeerida (vt näidisel „Personaliosakonna lauaarvutid). Võrguskeemi saab ruumipuudusel jaotada piirkondade (nt hoonete, korruste või seadmete teeninduspiirkondade) kaupa eraldi lehtedele.



Joonis 11 Võrguskeemi näidis

Lisaks siinsele joonisele on soovitav vaadata ka Jooniseid 2 ja 3.

6.2 KAITSEKAPPIDE SEADISTAMINE

Kaitsekappide seadistamisel tuleb järgida meetmeid:

- M 1.40 (M) Kaitsekappide sobiv paigutus
    1. Kontrollida paigalduskoha põranda kandevõimet.
    2. Kinnitada seina või põranda külge (varguskindlalt).
    3. Järgida tuleb olemasolevaid tootjanõuandeid nende sobivaks paigaldamiseks (nt vabad õhutusavad, kaablikarbikud).
- M 2.17 (M) Sisenemise reeglid ja reguleerimine
    1. Hoida sissepääsuõigusi omavate inimeste ring nii väike kui võimalik. Pääsuõigustega isikud peaksid teadma üksteise volitusi.
    2. Enne sisenemisloa andmist võõrastele isikutele (külalistele) kontrollida, kas see on vajalik.
    3. Väljastatud sissepääsuload dokumenteerida.
- M 2.21 (M) Suitsetamiskeeld
- M 3.20 (M) Kaitsekappide kasutamise juhised
    1. Töötajatele tuleb edastada vähemalt järgmised juhised:
        - Näidata kaitsekapi luku õiget kasutamist.
        - Serveri klaviatuuri tuleb kindlasti hoida serverikapis
        - Serverikapi kasutamise puhul tuleb selgitada, et sinna ei tohi panna hoiule mittevajalikke süttimisohtlikke materjale (nt pabermaterjalid).
        - Serveri varukoopiad sisaldavaid andmekandjaid tuleks hoida alati mõnes muus tuletõkketsoonis.
        - Konditsioneeriga varustatud serverikappide kasutamisel tuleks minimeerida aegu, millal serverikapp on avatud.
- M 1.15 (L) Aknad ja uksed suletud
    1. Aknad ja välisuksed (rõdud, terrassid) tuleb lukustada ajaks, mil ruumi ei kasutata.
- M 2.96 (M) Kaitsekappide lukustamine
    1. Kaitsekapid, mida ei kasutada, peavad olema lukustatud. Kui katkestatakse töö avatud kaitsekapi juures, tuleb ka lühiajalise lahkumise korral ruumist kaitsekapp lukustada.
- M 2.97 (M) Õige koodlukuprotseduur (kui on olemas)

6.3 TURVALÜÜSIDE/TULEMÜÜRIDE SEADISTAMINE

Turvalüüside ja tulemüüride seadistamisel tuleb järgida järgmisi meetmeid:

- M 2.76 (L) Sobivate filtreerimisreeglite valimine ja kehtestamine
- M 2.77 (L) Serverite integreerimine tulemüüri
- M 3.43 (L) Turvalüüsi administraatorite koolitus
- M 2.78 (L) Turvalüüsi turvaline kasutamine
- M 2.302 (M) Turvalüüsi kõrge käideldavuse tagamine
- M 4.47 (L) Turvalüüsi operatsioonide logimine
- M 4.100 (L) Tulemüür ja aktiivsisu
- M 4.101 (M) Tulemüür ja krüpteerimine
- M 4.222 (L) Turvaprokside õige konfigureerimine
- M 4.223 (M) Proksiserverite integreerimine turvalüüsi koostisse
- M 4.224 (M) Virtuaalsete privaatvõrkude integreerimine turvalüüsi koostisse
- M 4.225 (M) Logiserveri kasutamine turvalüüsil
- M 4.226 (L) Viiruseskännerite integreerimine turvalüüsi koostisse
- M 4.227 (M) Lokaalse NTP-serveri kasutamine aja sünkroniseerimiseks
- M 5.39 (L) Protokollide ja teenuste ohutu kasutamine
- M 5.46 (L) Autonoomsüsteemide installeerimine Interneti kasutamiseks (kohtvõrguühenduseta)
- M 5.59 (L) DNS-spuufingu tõrje
- M 5.70 (L) Võrguaadressi teisendus - NAT (Network Address Translation)
- M 5.71 (M) Sissetungi tuvastuse ja sellele reageerimise süsteemid
- M 5.115 (M) Veebiserveri integreerimine turvalüüsi koostisse
- M 5.116 (M) Meiliserveri integreerimine turvalüüsi koostisse
- M 5.117 (M) Andmebaasiserveri integreerimine turvalüüsi koostisse
- M 5.118 (M) DNS-serveri integreerimine turvalüüsi koostisse
- M 5.119 (M) Veebi-, rakendus- ja andmebaasiserveritega veebirakenduse integreerimine turvalüüsi
- M 5.120 (M) ICMP-protokolli käsitlemine turvalüüsis
- M 6.94 (L) Turvalüüside hädaolukorraks valmisoleku plaan

6.4 SERVERITE SEADISTAMINE

Serverite seadistamisel tuleb järgida järgmisi üldmeetmeid:

- M 2.32 (M) Piiratud kasutajakeskkonna loomine
- M 2.138 (L) Struktureeritud andmetalletus
- M 2.204 (L) Ebaturvalise võrkupääsu tõkestamine
- M 2.318 (L) Serveri turvaline installeerimine
- M 4.7 (L) Algparoolide muutmine
- M 4.15 (L) Turvaline sisselogimine
- M 4.16 (L) Konto- ja/või terminalipääsu piirangud
- M 4.17 (L) Tarbetute kontode ja terminalide blokeerimine
- M 4.40 (M) Arvuti mikrofoni volitamata kasutamise vältimine
- M 4.237 (L) IT-süsteemi turvaline aluskonfiguratsioon
- M 4.305 (L) Salvestusvõimaluste piiramine (Quotas-kvoodid)
- M 2.22 (L) Paroolide deponeerimine
- M 2.35 (L) Teabe hankimine turvaaukude kohta
- M 2.273 (L) Turvalisust mõjutavate paikade ja täiendite kiire paigaldamine
- M 4.24 (L) Järjekindla süsteemihalduse tagamine
- M 4.93 (L) Regulaarne tervikluse kontroll
- M 4.238 (M) Lokaalse paketifiltri rakendamine
- M 4.239 (M) Serveri turvaline käitus
- M 4.240 (M) Serveri testimiskeskkonna rajamine
- M 5.8 (M) Võrgu igakuine turvakontroll
- M 5.9 (L) Serveri logi
- M 6.24 (L) Hädaolukorra buutimismeedia loomine
- M 6.96 (L) Serveri ootamatuseplaan

Täiendavalt tuleb järgida operatsioonisüsteemi spetsiifilisi meetmeid, millele viidatakse moodulites B 3.1xx. Rakenduva mooduli määramisel on abiks lisas olev maatriks IT süsteemide kohta. Lisaks operatsioonisüsteemi spetsiifilistele nõuetele, tuleb rakendada ka serverisse paigaldatud (nii töötavate kui ka mitte töötavate) rakenduste spetsiifilisi nõudeid (moodulid B 5.*). Nende moodulite määramisel on abiks lisas olev maatriks.

6.5 LAUAARVUTITE SEADISTAMINE

Lauaarvutite seadistamisel tuleb järgida järgmisi üldmeetmeid:

- M 2.25 (L) Süsteemi konfiguratsiooni dokumenteerimine
- M 4.40 (L) Arvuti mikrofoni volitamata kasutamise vältimine
- M 4.237 (L) IT-süsteemi turvaline aluskonfiguratsioon

- M 2.273 (L) Turvalisust mõjutavate paikade ja täiendite kiire paigaldamine
- M 3.18 (L) PC kasutajate väljalogimiskohustus
- M 4.2 (L) Ekraanilukk
- M 4.3 (L) Perioodiline viiruseotsing
- M 4.4 (M) Draivipilude lukustus
- M 4.200 (L) USB-salvestite käsitlus
- M 4.238 (L) Lokaalse paketifiltri rakendamine
- M 4.241 (L) Kliendi turvaline käitus
- M 4.242 (M) Kliendi etaloninstalleeringu loomine
- M 5.45 (L) Veebibrauserite turve
- M 6.24 (L) Hädaolukorra buutimismeedia loomine
- M 6.32 (L) Regulaarne andmevarundus

Täiendavalt tuleb järgida operatsioonisüsteemi spetsiifilisi meetmeid, millele viidatakse moodulites B 3.2xx. Rakenduva mooduli määramisel on abiks lisas olev maatriks IT süsteemide kohta. Lisaks operatsioonisüsteemi spetsiifilistele nõuetele, tuleb rakendada ka arvutisse paigaldatud (nii töötavate kui ka mitte töötavate) rakenduste spetsiifilisi nõudeid (moodulid B 5.*). Nende moodulite määramisel on abiks lisas olev maatriks.

6.6 SÜLEARVUTITE SEADISTAMINE

Sülearvutite seadistamisel tuleb järgida samu meetmeid, mida ka lauaarvutite seadistamisel. Täiendavalt tuleb rakendada mobiilsusest tingitud meetmed:

- M 4.40 (L) Arvuti mikrofoni volitamata kasutamise vältimine
- M 5.121 (L) Turvaline side mobiilseadme ja töökoha vahel
- M 5.122 (L) Sülearvuti turvaline ühendamine kohtvõrguga
- M 1.33 (L) Kaasaskantavate IT-süsteemide hoidmine reisil
- M 1.34 (L) Kaasaskantavate IT-süsteemide hoidmine põhiasukohas
- M 1.35 (M) Sülearvutite ühisladustus
- M 1.46 (M) Vargusetõrjevahendid
- M 4.3 (L) Perioodiline viiruseotsing
- M 4.27 (L) Sülearvuti paroolkaitse
- M 4.28 (L) Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel
- M 4.31 (L) Toite tagamine mobiilkasutusel
- M 4.235 (L) Andmete seisu võrdsustamine sülearvutis
- M 4.236 (M) Sülearvutite tsentraalne haldus
- M 4.255 (M) Infrapunaliidese kasutamine

- M 5.91 (M) Internet-PC personaalse tulemüüri installeerimine
- M 6.71 (L) Mobiilse IT-süsteemi andmevarundus

6.7 PRINTERITE SEADISTAMINE

Printerite seadistamisel tuleb järgida järgmisi meetmeid:

- M 1.32 (L) Printerite ja koopiamasinate turvaline paigutus
- M 4.299 (M) Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel
- M 4.300 (M) Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve
- M 4.301 (L) Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele
- M 5.82 (L) Turvaline SAMBA kasutamine
- M 5.145 (L) Turvaline CUPSi kasutamine
- M 2.52 (L) Kulumaterjalide varude jälgimine ja täiendamine
- M 4.302 (L) Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimine
- M 4.303 (L) Võrgutoega dokumendiskännerite kasutamine
- M 4.304 (M) Printerite haldamine
- M 5.146 (L) Multifunktsionaalsete seadmete võrgust lahutamine
- M 6.105 (L) Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan

Juhul kui tegemist on võrguprinteriga (ka muud multifunktsionaalsed seadmed), mis käitub printserverina, tuleb rakendada ka serverite kohta käivaid meetmeid (vt. eelpool toodud juhendit).

6.8 VARUNDUSE KORRALDUSE JUHISED

Varundada tuleb (tähtsuse/olulisuse järjekorras):

1. Asutuse tööks hädavajalikke andmekogusid (nt. sotsiaalinfosüsteemi andmebaas, dokumendihoidla)
2. Andmeid käitlevate seadmete ja tarkvara logisid (enesekaitse, võimalus näha, kes, mida ja miks teha kui tekib probleeme nt. aasta pärast)
3. Teisi asutuse tööks vajalikke andmekogusid (nt. e-post)
4. Vähetähtsaid tööd abistavaid andmeid, mille kadu ei põhjusta olulist kahju/tööseisakut (nt. arvutite kasutajate profiilid (sh. My Documents ja Shared Documents))

5. Andmeid mitte käitlevate süsteemide töölogisid.
6. Süsteemide konfiguratsiooniseise (nt. arvuti ketta täiskoopia, millest saab vajadusel kiiresti arvuti kloonida).

Kõike ei ole vaja varundada, kuid varundada tuleb nii palju kui vähegi võimalik. Kindlasti tuleb korraldada punktides 1-3 kirjeldatud varundus.

Varunduse säilitamise periood peab vastama seaduste ja lepingutega sätestatud nõuetele.

- Operatiivkoopiat tuleb säilitada vähemalt seni, kuni samadest andmetest on loodud pikaajaline (väline) koopia, soovitavalt nädal kuni kuu kauem kui pikaajalise koopia tegemise aeg (nii kaitsete end välise koopia tegemisel tekkida võivate probleemide eest).
- Pikaajalist koopiat võiks säilitada vähemalt aasta, võimalusel kauem.
- Väikeste andmemahtude puhul sobib lühiajalise varukoopia andmekandjaks ka mälupulk ja pikaajalise koopia andmekandjaks DVD. **NB!** Koopia füüsiline ja digitaalne (nt krüpteerimine) turve tuleb siiski tagada.

Andmevarundus peab vastama järgmistele reeglitele:

- Olema regulaarne (nt igaöised operatiivkoopiad (koopiad, millele saab töökeskkonnast otse ligi – nt failide koopiad teises failiserveris või teisene domeenikontroller) ja iganädalased või igakuised suuremad (välised) koopiad (koopiad, mis hoitakse eraldi seifis originaalandmete ja operatiivkoopiatega erinevas füüsilises asukohas (nt teistes hoonetes)).
- Olema testitud (st andmete taastamist varukoopiatelt tuleks läbi teha vähemalt kord aastas ja varundamise korra muutumisel).
- Olema jälgitav (varundamisel tekkinud probleemid peavad olema administraatoritele varakult nähtavad).
- Olema planeeritud (varundusseadmeid ja andmekandjaid peab olema piisavalt varundatavate andmemahtudega hakkama saamiseks, varundustelt andmete taastamine peab mahtuma kindlatesse ajaraamidesse – nt 1h operatiivkoopialt, 1 päev väliselt koopialt).
- Varundatud andmed peavad olema piisavalt turvatud (nt krüpteeritud andmeid tuleb varundada vähemalt sama hästi krüpteeritult kui originaalandmeid, mitteavalike andmete varukoopiad ei tohi olla avalikud).

- Andmevarundused peavad olema originaalandmeid käitlevate süsteemide avarii (nt andmebaasimootori viga) korral ligipääsetavad ja kasutatavad.
- Andmete varundamine tuleb dokumenteerida (kes, millal, mida, kuhu ja kuidas varundas). Võimalusel kasutada automaatset varundamist, mis dokumenteerib end varunduse logides.

NB! Andmevarundus ei ole arhiiv! Olulised (e-)kirjad (otsused, taotlused, jms.) tuleb säilitada arhiivis pikaajaliselt.

6.9 OLEMASOLEVATE DOKUMENTIDE VASTAVUSSE VIIMINE ISKE MEETMETEGA

Järgnevas jaotises on kirjeldatud nõudeid, mis peaksid sisalduma juba olemasolevates siseregulatsioonides. KOVi vastava dokumendi eest vastutajal tuleb kontrollida, kas vastavad teemad on dokumendis käsitletud. Kuna mitmed teemad võivad olla kas samaaegselt või erinevates KOV-des erinevates dokumentides kirjeldatud, siis on siinkohal soovitus omavahel kontrolli tulemeid kooskõlastada ja mitte dubleerida samu nõudeid erinevates regulatsioonides. Nii on edaspidi lihtsam dokumentatsiooni kaasajastamine.

6.9.1 Sisekord

Sisekord kajastab enamasti füüsilise turbe meetmeid. Asutusel tuleb kontrollida, kas sisekorras või mõnes analoogses siseregulatsioonis on kajastatud vähemalt järgmised ISKE meetmetest.

M 1.6 Tuletõrje-eeskirjade täitmine

Tuleohutuse eest vastutav töötaja

Tuleohutuseeskirjad ja nende täitmine, tulekustutusvahendid, nende kasutamise juhendamine jm seonduv. Enamasti kõigis Eesti asutustest küllaltki korrektselt täidetud.

M 1.15 Aknad ja uksed suletud

- Kas on olemas korraldus akende ja välisuste sulgemiseks ruumist lahkumisel?

- Kas kontrollitakse reeglipäraselt akende ja uste lukustamist pärast ruumist lahkumist? Nt viimane lahkuja peab kontrollima. Koristaja lisaülesanne. Siin võib olla ka viide lukustatavatele dokumendi kappidele.

M 1.18 Valve- ja tuletõrjesignalisatsioon

Kas on olemas ohtude avastamise, ohusignaalide edastamise ja häiresignalisatsiooni kontseptsioon ning kas kasutamisel toimub selle kohandamine muutustega? Põhimõtted, kuidas ja milleks on paigutatud, kes on teavitatavad isikud, kuidas tööle rakendatakse, kellele kuidas koode jaotatakse, millal vahetatakse, kuidas käitutakse grupikoodidega jms sisemised kokkulepped.

- Kas toimub signalisatsiooniseadme reeglipärane hooldus ja kontroll? Kelle tööülesanne on seda korraldada?

M 1.23 Lukustatud uksed

- Kas kontrollitakse pisteliselt büroode lukustamist, kui sealt lahkutakse – ka lühiajaliselt, eriti kui kogu hoone on nn avatud tsoon mitte vaid oma töötajatele?

- Kas töötajatele antakse korraldus büroo lukustamiseks nende äraolekul?

M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil

Soovitav on koostada mobiilsete IT-süsteemide kasutajate jaoks infoleht, mis sisaldab tähtsamaid nõuandeid ja ettevaatusabinõusid seadmete nõuetele vastavaks hoidmiseks ja turvaliseks transpordiks.

- Kas kaasaskantavate IT-süsteemide kasutajate tähelepanu juhitakse seadmete õigele hoidmisele?

M 1.34 Kaasaskantavate IT-süsteemide hoidmine põhiasukohas

- Kuidas hoitakse kaasaskantavaid IT-süsteeme büroodes? Nende füüsiline turve – kütteseadmetest ja veetorudest eemal, juhtmed kasutajatele ohutult ja nende ekspluatatsiooni säästvalt, ekraan eemal võõraste vaateväljast (nt aknad 1. korrusel, kliendid, töötajad teistest pääsugruppidest), nn klienditsoonis kasutada lukke (nt Kensingtoni lukk), või hoida mitte nähtaval (fotoaparaadid, diktofonid, projektorid vms – spetsiaalsetes kappides konkreetsete inimeste vastutusel)

M 1.45 Äridokumentide ja –andmekandjate sobiv talletus

Kas töötajaid on instrueeritud, et kõrge kaitsevajadusega andmeid sisaldavaid dokumente ja andmekandjaid tuleks hoida lukustatud hoiukohas?

M 1.61 Mobiilse töökoha sobiv valimine ja kasutamine

- Kas töötajaid informeeritakse, millele nad mobiilse töökoha valikul ja kasutamisel peavad tähelepanu pöörama? Nt juhtmed kasutajatele ohutult ja nende ekspluatatsiooni säästvalt, ekraan eemal võõraste vaateväljast, niiskuse ja liigse päikesepaiste vältimine, lastele või muudele isikutele kättesaamatult, turvaliselt stabiilsel pinnal, et vältida füüsilisi kahjusid.

M 2.6 Sissepääsuõiguste andmine

Enne sissepääsuõiguste jagamist töötajatele tuleb määratleda erinevate ruumide turvaklassid. Seejärel tuleb kindlaks teha, milliseid sissepääsuõigusi töötajad vajavad oma tööülesannete täitmiseks (sh arhiiv, serveriruum, seadmetekapp, dokumentide kapp, võtmete kapp, printeri ruum jne). Pääsuõigused tuleb fikseerida taasesitatavalt.

Sarnaselt oma töötajaskonnale tuleb määrata ka väljastpoolt tuleva personali ja külastajate sissepääsuõiguste jagamise ja tagasivõtmise kord.

M 2.14 Võtmete (ja kaartide) haldus

- Kuidas on reguleeritud võtmete haldamine? Vt M2.6 määratlusi. Missuguseid kohustusi võtme omamine kaasa toob – paljundamine, kaotamine, tagastamine, edasiandmine? Kuidas toimitakse pikaajalise tööst eemalolemise korral (nt lapsehoolduspuhkus), ootamatu lõplik töölt eemale jäämine (nt surm).

M 2.16 Välispersonali ja külastajate valve ja saatmine

Kõikidele töötajatele tuleb selgitada, et võõrad isikud, keda kohatakse ilma saatjata ametiasutuse või ettevõtte territooriumil ringi liikumas, tuleb alates kohtumise hetkest oma hoolitsuse ja järelvalve alla võtta.

- Kas töötajaid on korduvalt teavitatud sellest, millist käitumist neilt oodatakse?

M 2.17 Sisenemisreeglid ja reguleerimine

Sisenemine kaitset vajavatesse majaosadesse ja ruumidesse peab olema reguleeritud ning seda tuleb kontrollida. (Nt serveriruum, seadmekapp, arhiiv, tehniline ruum nt koopiamasinate ja printerite tööks)

M 2.21 Suitsetamiskeeld

M 2.37 Korrastatud töölaud

Kõik töötajad peavad ühtemoodi hoolsad olema oma töökoha kontrollimisel, et veenduda, et tundlik informatsioon ei oleks vabalt juurdepääsetav, ning et andmete kättesaadavus, nende konfidentsiaalsus ja terviklus ei kannataks.

M 2.333 Nõupidamis-, ürituste- ja koolitusruumide turvaline kasutamine

Igas organisatsioonis peaks olema niisuguste ruumide kasutamiseks kehtestatud kindlad reeglid. Reeglid peaksid muuhulgas sisaldama kasutajatele suunatud üldisi käitumisreegleid, samuti nii statsionaarselt paigaldatud kui ka kaasavõetud seadmete kasutusreegleid.

- Ruumi kasutuse kooskõlastamine, vastutus ürituse korraldajal, konfidentsiaalsete materjalide kõrvaldamine nõupidamiste ruumist (eelmiste koosolekumaterjalid pabertahvlil, jaotusmaterjal, esitlusmaterjal esitlusarvutis (selle puhastamine)), sisevõrgupääsu tõkestamine, vajadusel alamvõrk.

6.9.2 Asjaajamiskord

KOV peaks kontrollima, kas asjaajamiskorras või mõnes muus tööregulatsioonis on vastavad viited järgnevatele teemadele olemas. Teemad on esitatud ISKE meetmete kaupa koos lühikese kontrollküsimuse või selgitusega. Täpsustamise vajaduse ilmnemisel tuleb lähtuda meetme pikast selgitusest ISKE meetmete kataloogis. Meetmete kirjelduste kordumisel erinevates dokumentides tuleb tagada nende esituse kooskõlalisus.

M 1.36 Andmekandjate transpordieelne ja –järgne turvaline säilitus

- Kas töötajate tähelepanu on juhitud asjaolule, et transporti ootavaid andmekandjaid (nii paberid, mälupulgad, CD-d, DVD-d, mälukaardid või muu media) ei hoitaks nii, et need oleks kõigile juurdepääsetavad.

M 1.60 Arhiivi-andmekandjate asjakohane säilitus

- Kas hoiutingimused on arhiivisüsteemide kasutusjuhendis dokumenteeritud?

- Kas hoiutingimuste mittejärgimise puhuks on välja töötatud eskalatsiooniprotseduurid?

Teema peaks kajastuma eelkõige arhiivijuhendis või selle analoogis.

M 2.42 Võimalike suhtluspartnerite määramine

- Kas võimalikud kommunikatsioonisuhted on reguleeritud? Kellele, kuidas ja millist informatsiooni jagatakse, kas jäävad maha taasesitatavad jäljed? Kirjalikud vastused, info edastamine telefonitsi, info edastamine kohapeal suuliselt, info edastamine teiste kuuldeulatuses. Info konfidentsiaalsuse turbeosaklassist sõltuvus.

- Kas mainitud ülevaateid uuendatakse regulaarselt? Arvestada olukordade ja seadusandluse muudatusi.

M 2.43 Andmekandjate õige märgistus edasiandmiseks

- Kas edasiantavate andmekandjate märgistamisreeglid on ette antud?

- Kas märgistamise reeglistikust kinnipidamist kontrollitakse pisteliselt? (sh nt info turvaklassi kohta) nt sisse ja väljaminevate kirjade tähistused.

M 2.44 Andmekandjate pakkimine edasiandmiseks

- Kas erinevate andmekandjate turvaliseks transportimiseks vajaminevad pakendid on organisatsiooni poolt kasutamiseks ette kirjutatud ning kas neid on piisavas koguses olemas? Nt asutuste vaheline andmete transport – nii digitaalne kui paberkandjal.

- Kas transportimisel kasutatavad pakendid võimaldavad adressaadil kontrollida, et pakendi sisuga ei oleks manipuleeritud?

M 2.45 Andmekandjate üleandmine

Kindlaks tuleb määrata sobilik saatmisviis. Sealjuures on tarvis pöörata põhitähelepanu andmekandja liigile ja sellel olevate andmete kaitsevajadusele.

M 2.47 Faksi eest vastutaja

Iga faksiseadme kohta tuleb määrata vastutav isik, kelle tööülesannete hulka kuuluvad järgnevad tegevused:

- sissetulnud fakside edastamine nende adressaatidele,

- faksiseadmele vajaminevate kulumaterjalide varustamise koordineerimine,

- faksi kulumaterjalide korrakohane hävitamine,

- faksiseadme jääkinfo korrakohane kustutamine enne seadme hooldus- või remonditöid,

- kohalviibimine hooldus- ja remonditööde juures (vt M 2.4 Hoolduse ja remondi eeskirjad),

- süsteemi sisestatud adressaatide ja protokollide pisteline kontroll, eriti pärast hooldus- ja remonditöid,

- olla kontaktisik faksi kasutamisel esinevate probleemide korral.

M 2.48 Faksioperaator

Töötajatele tuleb õpetada korrektset faksiseadmega ümberkäimist ning koos sellega ka IT-turvameetmete järgimist. Mõistlikum on jätta see ühe konkreetse inimese tööülesandeks.

M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid

IT-süsteemide või andmekandjate kasutamine väljaspool maja, nt ametireisidel või kaugtöös.

Tuleb kindlaks määrata,

- milliseid IT-komponente või andmekandjaid tohib majast välja viia (sülearvutid, fotoaparaadid, mälupulgad, diktofonid jne),

- kes tohib IT-komponente või andmekandjaid majast välja viia (pigem erand kui reegel, erand vajab aga eraldi kinnitamist. Andmete omanik peab teadma, mis potentsiaalselt võib andmetega juhtuda,

- milliseid põhilisi IT-turvameetmeid peab seejuures järgima (viirustõrje, konfidentsiaalsete andmete krüpteerimine, säilitamine, sülearvuti kasutamine avalikus kohas jne.),

- kas reeglid on kehtestatud igat liiki IT-komponentide kaasavõtmise kohta? (nt, mälupulgad, sülearvutid vms, eraldi kokkuleppeid vajavad aga paberkandjad, sh fotod)

- kas väljaspool maja kasutatavate IT-komponentide kasutajatele tutvustatakse reegleid, millest nad peavad kinni pidama?

- kas väljaspool maja kasutatavate IT-komponentide kasutajate tähelepanu juhitakse sellele, et komponente tuleb hoida nii, nagu on ette nähtud?

M 2.393 Infovahetuse reguleerimine

- Kui suur on selle kaitsevajadus (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus)? Igal turvaklassil/astmel oma üldine reegel. Nt S2 osaklassiga teemad ei tohi lekkida väljapoole konkreetse kasutajate grupi piire. Vastava info asutusest

väljaandmisel tuleb veenduda vastaspoole õiguses seda infot saada, vajadusel peab olemas olema taasesitatav luba andmesubjektilt.

- Kellega tohib informatsiooni vahetada (vt M 2.42 Võimalike suhtluspartnerite määramine)? Kellele ollakse andmeandja, kellele andmesaaja.

- Kuidas seejuures informatsiooni kaitsta (vastavalt IKS ja AvTS nõuetele).

Kõik töötajad peavad olema teadlikud, et nad vastutavad siseinfo (siinhulgas igasuguse tööülesandeid täites teatavaks saanud info) kaitsmise eest nii asutuses töötamise ajal kui ka töösuhte lõppemise järgselt – enamasti on see määratletud ametijuhendiga.

M 4.64 Edastatavate andmete verifitseerimine enne edastamist

Jääkinformatsiooni kõrvaldamine

- Kas arvutikasutajaid on informeeritud failides sisalduvast jääkinformatsioonist tuleneda võivatest ohtudest ?

- Kas arvutikasutajatele on selgitatud kiirsalvestusvalikute kasutamisest tuleneda võivaid ohte ?

Lisaks nt edasi saadetavates kirjades kontrollida, et ekraani pildist väljajääv osa kuulub saadetava meili juurde.

M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist

Kas andmekandjate vahetamise eest vastutav isik tunneb füüsilise kustutamise meetodit?

- Kas füüsiliseks kustutamiseks kasutatavad programmid on nende töötajate käsutuses?

- Kas kaitsmist vajava informatsiooni saajaid on edastatavate andmete kaitsmise vajadusest informeeritud?

Kui kasutatakse sisseostetavaid teenuseid, siis veenduda lepingus sisalduvatest kohustustest konfidentsiaalsusele ja sanktsioonidele.

M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel

- Kas kasutatakse võimalikult uut viirusetõrjeprogrammi?

- Kas vahetamiseks mõeldud andmeid kontrollitakse enne nende vahetamist viiruste suhtes?

- Kas selle kontrollimise protokoll edastatakse saatjale?

- Kas saadud faile ja andmekandjaid kontrollitakse enne nende arvutisse laadimist viirustega nakatatuse suhtes?

M 4.34 Krüpteeringu, kontrollsummade või digitaalallkirjade kasutamine

- Kas konfidentsiaalsuse või tervikluse kaitsmiseks antakse töötajate käsutusse krüpteerimisprogrammid või kontrollsumma meetodid? (nt digitaalallkirjastamine, digitempel)

- Kas andmete edastamise eest vastutavaid töötajaid on võtmete nõuetelevastavast kasutamisest informeeritud?

- Kas konfidentsiaalsuse/tervikluse kaitse tuleb tagada ainult andmete edastamisel/transportimisel või ka saaja või saatja süsteemis? Kuidas vastav info edastatakse, nt vastava kirja jalusega? Üks võimalus on:

HOIATUS: Käesolevas kirjas ja selle võimalikes lisades sisalduv informatsioon on määratud ainult kirja adressaatidele ning võib omada konfidentsiaalset iseloomu. Kui olete selle kirja saanud eksituse tõttu, siis on kogu selles sisalduva informatsiooni avaldamine täielikult või osaliselt, mistahes kujul või meedias, selle paljundamine, sellele viitamine või selle mistahes viisil kasutamine Teile rangelt keelatud. Sellisel juhul palume teavitada saatjat kirja saabumisest valele aadressile ning kustutada koheselt käesolev kiri koos võimalike lisadega kõigist Teie valduses olevatest infosüsteemidest ja -kandjatelt.

M 4.35 Edastatavate andmete verifitseerimine enne nende ärasaatmist

- Kas vahetatavaid andmekandjaid kontrollitakse enne andmete saatmist selles osas, kas soovitav informatsioon on andmekandjalt täielikult rekonstrueeritav? Sh sobilik formaat.

- Kas elektroonilised andmekandjad kustutatakse enne järgmist kasutust füüsiliselt, kui eelnevalt olid sellele muud andmed salvestatud?

M 3.55 Konfidentsiaalsuslepingud

Sisemistes regulatsioonides tuleb fikseerida, milliseid andmeid tuleb käsitleda konfidentsiaalsetena, nii ka kõigis sõlmitavates lepingutes,

- kui pikk on sõlmitavate konfidentsiaalsuslepete kehtivusaeg,

- mida tuleb teha sõlmitud konfidentsiaalsuslepete lõppemisel, nt kas vastavad andmekandjad tuleb hävitada või tagastada ,

- kuidas on reguleeritud informatsiooni omandiõigused,

- millised ettekirjutused kehtivad vajadusel konfidentsiaalse info kasutamise ja edasiandmise kohta täiendavatele partneritele,

- millised on konfidentsiaalsusleppe rikkumise tagajärjed.

- Kas välistele töötajatele pandi enne juurdepääsu võimaldamist konfidentsiaalsele infole kohustus vastava infoga konfidentsiaalselt ümber käia?

- Kas konfidentsiaalsuslepetes arvestatakse piisavalt kõikide oluliste aspektidega, mis tagaksid organisatsiooni siseinfo piisava kaitse?

6.9.3 Täiendused ametijuhenditesse

Ametijuhendis või muus sisemises regulatsioonis tuleb fikseerida, mida loetakse konfidentsiaalseks infoks. KOV-de puhul käib siia eelkõige

- isikuandmed ja delikaatsed isikuandmed.
- AvTS §35.

KOV-de erinevate ametnike ametijuhendid peavad sisaldama infot, milliste andmekogudega vastav töötaja kokku puutub.

Vastutusena tuleb fikseerida vähemalt järgmised klauslid, mis sisaldaksid analoogset infot:

- Tööülesannete nõuetekohase, õigeaegse ja korrektse täitmine.
- Töö käigus esitatud ja koostatud andmete õigsuse ning seaduslikkuse ja otstarbekus.

- Töövahendite ja muude materiaalsete väärtuste säästliku plaanimise ja sihipärase ja heaperemehelik kasutamine.
- Töö tõttu teatavaks saanud ametisaladuse, ärisaladuse, teiste inimeste perekonna- ja eraellu puutuvate andmete ning muu konfidentsiaalse informatsiooni kaitsmise ja hoidmise eest.
- Personaalsete kasutajakoodide ja salasõnade hoidmise eest.
- Asutuse sisemiste regulatsioonide täitmise eest.
- Tööülesannete täitmisel esinevate õigusrikkumiste eest vastutab seaduses ettenähtud korras.

