EESTI KOHALIKU OMAVALITSUSE IKT TARISTU MIINIMUMNÕUDED

Eesti Maaomavalitsuste Liit 2017

Henri Pook | Nevel Paju

SISUKORD

1. Käsitlusala 3
2. Soovituslik mudel tulevikuvõrgu ehitamisel KOV-is 4
3. Süsteemi suund 4
4. Internetiühendus 6
5. LAN kohtvõrk 7
6. Tulemüür 8
7. Võrgulüliti 9
8. Serverid 9
9. Arvutitöökohad 10
10. Kasutajate haldusteenus 10
11. Lõppseadmete haldus 11
12. E-posti teenus 11
13. Viirusetõrje 11
14. Varukoopia 11
15. PBX (VOIP) 12
16. Failihaldus 12
17. KOV IKT võrgu kohustuslik dokumentatsioon: 12

1. KÄSITLUSALA

„Infoühiskonna arengukava 2020“ sissejuhatuses on öeldud, et vältimaks vanasse tehnoloogiasse kinnijäämist viiakse ellu avalike e-teenuste ja neid toetavate IT-lahenduste ümberkujundamise reform. Eesti avalikud (e-)teenused peavad olema kaasajastatud ja ühtsetele kvaliteedinõuetele vastavad. Lisaks rakendatakse n-ö *no legacy* põhimõtet – see tähendab, et avalikus sektoris ei tohi olla olulise tähtsusega info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) lahendusi, mille vanus on vanem kui 13 aastat.[1]

Käesolev soovituslik mudel on koostatud selleks, et IKT süsteeme üles ehitades järgitaks teiste kohaliku omavalitsuse üksuse asutuste (edaspidi *KOV, omavalitsus*) ja ülejäänud Eesti riigiasutuste üldpilti ning turvalisust. Miinimumnõuded kehtestatakse eesmärgiga tagada KOV asutuste IKT-taristu ja sellega seotud teenuste nõuetekohane toimimine ning arendamine.

Kohaliku omavalitsuse üksuste haldusreformi perioodil on tekkinud paratamatu vajadus analüüsida liituvate valdade tuleviku IKT taristut ning leida jätkusuutlik ja kaasaegne lahendus selle haldamiseks. Miinimumnõuded kehtestatakse kooskõlas „Infoühiskonna arengukava 2020“ põhimõtetega. Kui IKT taristu on ülesehitatud kaasaegselt ja standardselt, võimaldab see hiljem taristu süsteemset haldamist, mis väldib planeerimatuid väljaminekuid ning vähendab turvariske.

IKT taristute ehitamisel ja haldamisel peavad kõik omavalitsused täitma infosüsteemide turvameetmete süsteemi ISKE (edaspidi *ISKE*) nõudeid.

KOV IKT taristu ja teenuste tingimuste kehtestamise ja täitmise eest vastutab asutuse juht.

Kõik kasutatavad IKT taristud peavad olema ajakohaselt dokumenteeritud, jälgitavad ja hallatavad.

Hetkel on tehnoloogia areng selline, kus kõik seadmed ei pea olema kohapeal, vaid piisavalt hea internetiühenduse korral võib võtta serverite ja võrgukomponentide majutamiseks kasutusele näiteks Riigipilve.[2] Ka väliste teenuste osas on võimalik viia vastavad infosüsteemid lokaalvõrgust välja, kui ISKE nõuded on majutaja ja teenusepakkuja poolt täidetud. Infosüsteemide väljaviimine vabastab omavalitsuse nende majutusega kaasneva ISKE nõuete kehtestamisest, kuna see on sageli liialt kulukas. Muidugi on ka erandeid, mille puhul ei ole infosüsteemide väljaviimine võimalik. Seda võivad tingida võrguühenduse eripärad, näiteks vallamajades pole piisavalt kiiret andmesidet ning tänu sellele mahukaid sisekasutuses olevaid andmekogusid ei saa välja viia (näiteks failiserverid).

[1] http://infoyhiskond.eesti.ee/files/Infoyhiskonna_arengukava_2020_f.pdf

[2] Pilvelahendust saab kasutada ainult juhul kui majutatavate komponentide ISKE turvaklassid on täidetud.

Juhul kui väliseid teenuseid majutavaid andmekogusid peetakse lokaalvõrgus, tuleb nendele andmekogudele kehtestada ISKE turvaklassid. Käesolev mudel kirjeldab ISKE turvanõuetest lähtudes sellist lokaalvõrku, kuhu pole majutatud väliselt ligipääsetavaid andmekogusid.

2. SOOVITUSLIK MUDEL TULEVIKUVÕRGU EHITAMISEL KOV-IS

Tulevikuvõrgu ehitamise etapid:
2.1. kaardistada ja koostada praeguste võrkude joonised, sealhulgas ka nõrkvoolu võrgukaabeldus (alusdokumendid: hoonete ehitusjoonised, plaanid). Joonisele märgitakse kogu IKT taristu (serverid, tulemüürid, võrgujaoturid, arvutid, printerid jne);
2.2. võrrelda olemasolevaid kaardistusi käesoleva mudeliga komponentide kaupa ning teha kindlaks, millised seadmed ei täida tulevikuvõrgus enam neile pandud ülesandeid;
2.3. koostada käesoleva mudeli soovitusi järgides uus tuleviku omavalitsuse IKT taristu joonis, mille lisatakse vajaminevate komponentide kirjeldused ja kogused ning koostatakse eeldatav maksumuse eelarve.

3. SÜSTEEMI SUUND

3.1. Liitvõrku ehitades tuleb teha valik kolme peamise arhitektuuri vahel: pilv, hübriid, kohapealne.

3.2. Pilveteenus: kogu serveripargi (kasutajate haldus, e-post, failid, arvutite haldus, viirusetõrje keskhaldus jne) osa on majutatud pilveteenust pakkuva majutaja juures (näiteks Riigipilv). Kohapeal on ainult töökoha arvutid, võrgujagajad, tulemüür, printerid.

Käesolev mudel ei keskendu pilvelahenduse kirjeldamisele. Kui on soov tellida IKT võrguhaldus läbi pilveteenuse, siis on vaja arvestada teenuse hankimisel käesoleva mudeli põhimõtetega.

3.3. Hübriidlahendus: osa serveritest on kohapeal ning osa pilves. Näiteks: kohapeal on kasutajate haldus ja failiserver ning pilves dubleeriv kasutajate haldus, e-post ja varukoopia. Mõistlik on kaaluda hübriidlahendust siis, kui vallavalitsusse tulev internetiühendus ei ole piisava kiirusega, et kogu lahendusele rakendada pilveteenust.

Hübriidlahendusega on tegemist ka siis, kui pilves on ainult e-post, mis on seotud lokaalvõrgus oleva kasutajate haldusega, kui see on ISKE nõuetega kooskõlas (näiteks Office365 mis on seotud AD`ga).

3.4. Lokaalne süsteem: kõik lokaalvõrgu serverid asuvad omavalitsuse kontrolli all olevas serveriruumis või omavalitsuse hoonetes olevates serveriruumides.

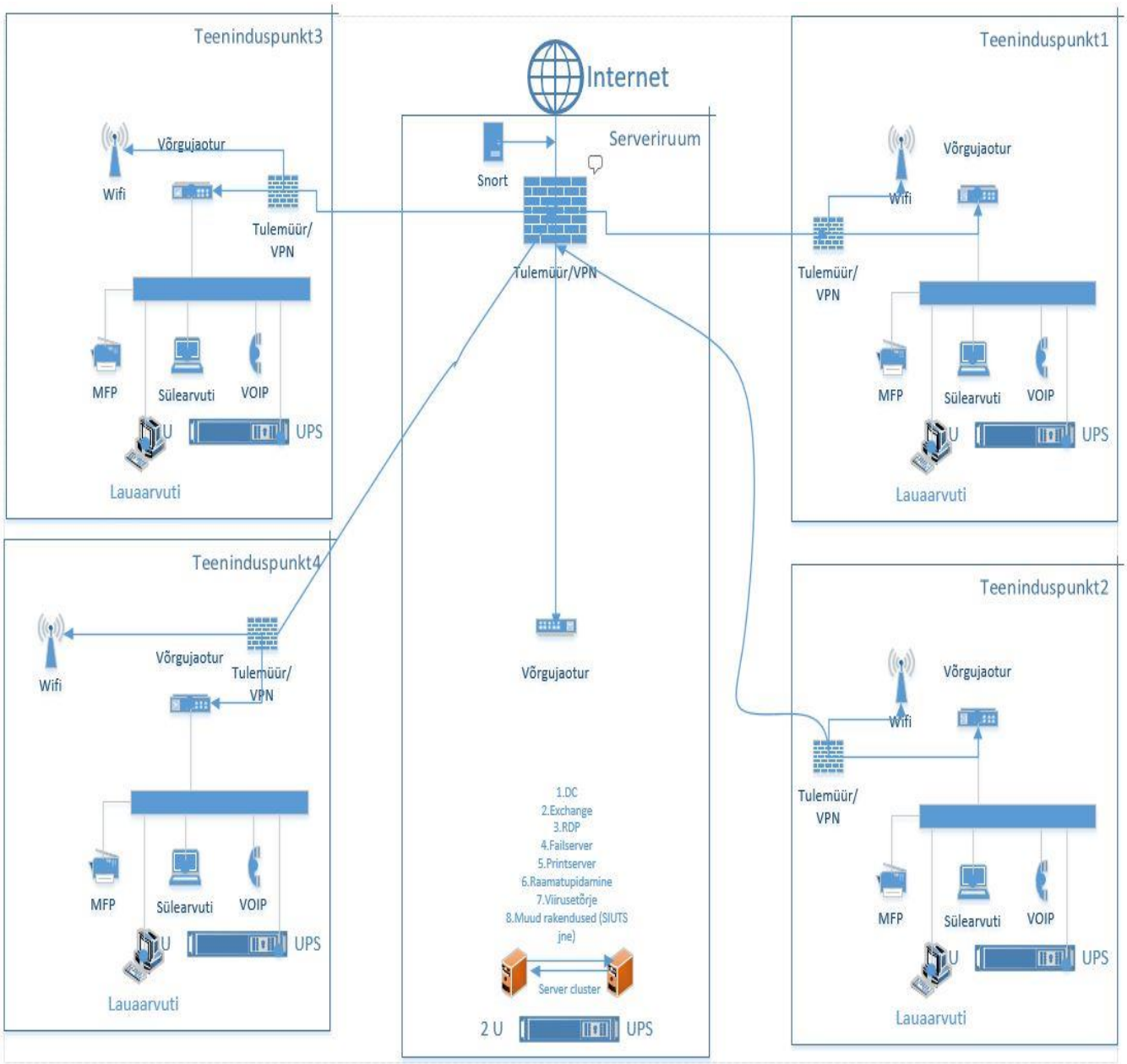
3.5. Otsustada tuleb, kas planeeritavad töökoha arvutid hakkavad põhinema vabavaralisel või litsentseeritud tarkvara lahendusel (näiteks Microsoft või Linux). Selle otsuse tegemisel on kõige

olulisem aspekt võrguhaldamise jätkusuutlikus (näiteks kas IT-spetsialisti või teenusepakkuja muutumisel suudetakse probleemideta arvutitöökohtade ja võrguhaldust jätkata).

3.6. Võrgu planeerimisel on kindlasti vaja analüüsida, kas võrku liituvad hiljem ka KOV hallatavad asutused (näiteks raamatukogud, lasteaiad jt). Võrgukomponentide ja serverite hankimisel tuleb sellisel juhul arvestada nende skaleeritavuse ja kasutusajaga.

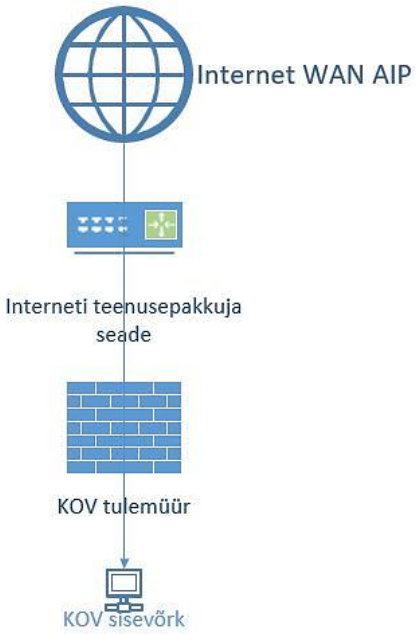
3.7. Tänapäeval ei pea enam olema füüsilist töökohta (töölauda ja sellel olevat konkreetse kasutajaga seotud arvutit). Seetõttu tuleb mobiilsete töökohtade loomine planeerida võrguarhitektuuri osana.

Lokaalse võrgu joonis:



4. INTERNETIÜHENDUS

4.1. Internetiühenduse joonis



4.2. Vallamajas ja teeninduspunktides peab internetiühendus olema staatiliste IP-dega, et tagada tulemüüride, serverite ja muude võrguseadmete turvaline hallatavus.

Internetiliiklus välismaailmaga peab välja liikuma ühest punktist, kuhu on paigaldatud võrgu analüsaator (SNORT; IDS vms), et tagada informatsioon võrgus toimuvast.

Kui liituva valla vallamajas ei ole piisava kiirusega interneti ühendust, siis tuleks kontrollida, kas mõnes omavalitsuse teeninduspunktis on nõuetele vastava ühenduse võimalus. Sellisel juhul soovitame serveriruumi viia sobiva internetiühendusega teeninduspunkti.

4.3. KOV internetiühenduse vajadus sõltub tehnoloogia kasutamise tasemest. Eeldame et IKT on aktiivses kasutuses ning tööprotsesside osa.

4.4. Soovitus interneti paketi valikul:

kuni 10 töötajat→ minimaalselt 30 Mbit/s alla- ja üleslaadimine[3];
kuni 30 töötajat → minimaalselt 50 Mbit/s alla- ja üleslaadimine;
kuni 50 töötajat → minimaalselt 100 Mbit/s alla- ja üleslaadimine;
50 ja rohkem töötajat → minimaalselt 1 Gbit/s alla- ja üleslaadimine.

[3] Sümeetriline ühendus on oluline, kuna teeninduspunktide välisühendus liigub läbi keskse pöördumispunkti.

4.5. Arvestada tuleks ka ajutiselt võrku sisenevate kasutajatega, näiteks volikogu liikmed, wifi jne. Kui sisevõrgus olevate serverite kaudu pakutakse väliseid teenuseid (näiteks koduleht, erinevad registrid), siis tuleb kaaluda interneti ühenduse kiiruse tõstmist vastavalt teenuse vajadusele. [4]

4.6. Välisühenduse tellimisel on käideldavuse seisukohast oluline rikete kõrvaldamise aeg. Oluline on tagada tavapärasest kiirem rikete kõrvaldamine asutuse tööajal.

5. LAN KOHTVÕRK

5.1. Kohtvõrgu kaabeldus
Statsionaarsete töökohtade korral on mõistlik kasutada kaabeldatud ühendust, mis tagab stabiilse ühenduse tööks vajalike infosüsteemide ning failide liigutamiseks. Arvuti kaabeldus peab vastama vähemalt ISO/IEC11801 standardile. Võrguehitustöid tellides on mõistlik sätestada see nõue lepingus.
5.2. Uue kaabelduse ehitamisel on mõistlik kasutada tänapäeval levinud CAT6 standardit. Võrgujaotlate vahel on soovitatav kasutada CAT6 või fiiber-optilist kaabeldust, et tagada piisav andmevahetus võrgujaoturite ja võrguseadmete vahel.

5.3. Seinal, põrandal või laes olev kaabel tuleb kaitsta karbikuga.

5.4. Kaabel peab olema otsastatud pistikupesaga ning markeeritud ja kirjalikult dokumenteeritud.

5.5. Wifi kasutamine

5.5.1. Wifi kasutamine KOV sisevõrgus ei ole soovitatav kuid juhul kui see osutub vajalikuks (näiteks mobiilsed tööjaamad) siis tuleks sisevõrgus kasutada 802.1x protokollistikku või jagada sisevõrku läbi VPN-i.

5.5.2. Avaliku wifi võrku sisenejad võtavad vastutuse oma tegevuse eest ja vajadusel peab olema võimalik käivitada kasutajate autentimine.

5.5.3. Täpsemalt on wifi kasutamise riske ja nõudeid kirjeldatud https://www.ria.ee/ee/wifi-kasutamisest.html.

5.6. Juhtmevaba interneti pääsupunkt (*Access Point*) on seade, mis võimaldab juurdepääsu internetile või muule andmesidevõrgule. Pääsupunktide valimisel on oluline IEEE 802.11 b/g/n standardite tugi. 802.11b on mõtet lisada nõudena vaid siis, kui KOV-is on piisavalt palju wifi seadmeid, mis toetavad vaid 802.11b standardit ehk mis on vanemad kui 10 aastat ja toodetud

[4] Kui on KOV`i lokaalvõrgus on andmekogu mis osutab väliseid teenuseid siis tuleb mõelda dubleerivale ühendusele, et tagada käideldavuse nõuded.

enne 2003. aastat. Kui sellised seadmed vahetatakse igal juhul lähiajal välja või puuduvad need sootuks, siis tasub selle standardi nõudest loobuda, kuna need seadmed vähendavad wifi võrgu kiirust halvemal juhul kuni 75% võrreldes 802.11n MIMO2x2 tavapärase konfiguratsiooniga.

5.7. Kaasaegsed wifi ruuterid võimaldavad kasutada samaaegselt 2.4GHz ja 5GHz sagedusala. See tagab suurema kliendiseadmete arvu sama tugijaama levialas ning madalamal andmevahetus-kiirusel (802.11b/g) töötavad seadmed ei mõjuta nii palju uute, kiiremat andmeedastuse standardit (802.11n) kasutavate seadmete kiirust.
5.8. Oluline on seadme vähemalt 300Mbps andmeside läbilaskevõime.
5.9. Turvalisuse tagamiseks on oluline WPA2 Personal+Enterprise turvatoe olemasolu.[5].

6. TULEMÜÜR

6.1. Tulemüür on oluline organisatsiooni IKT turvapoliitikate rakendamise punkt. Selle abil saab lubada ja keelata erinevaid tegevusi KOV sisevõrgu või erinevate sisevõrkude ning avaliku interneti vahel. See võimaldab ka saada ülevaate kohtvõrgus toimuvast. Tulemüüri abil on võimalik peatada erinevaid rünnakuid kas automaatselt, erinevate tüüpreeglite kirjeldamise kaudu või käsitsi, reageerides konkreetsele olukorrale vahetult tulemüüri kasutajaliideselt.

6.2. Soovituslikud nõuded tulemüürile:
6.2.1. jõudlus: kuni 100 Mbps internetiühenduse korral peab tulemüüri jõudlus olema vähemalt 150Mbps. Kuni 1 Gbit internetiühenduse korral peaks tulemüüri jõudlus olema 1.2 Gbps;
6.2.2. tehnoloogia: olekuteadlik tulemüür [6];
6.2.3. vähemalt üks laivõrgu (WAN) port. Vähemalt 4 kohtvõrgu (LAN) porti ja 1 demilitariseeritud tsooni (DMZ) port või vähemalt 5 konfigureeritavat porti;
6.2.4. avatud vormingus logimine ja ühilduvus enamlevinud haldusrakendustega;
6.2.5. portide peegeldamise funktsioon: mitu-ühele;
6.2.6. enimlevinud internetiprotokollide tundmine (HTTP, HTTPS …);
6.2.7. IP aadresside transleerimise tugi (NAT);
6.2.8. turvaliste virtuaalvõrkude ehitamise võimalused (VPN);
6.2.9. IEEE 802.1Q virtuaalsete kohtvõrkude (VLAN) tugi;
6.2.10. ribalaiuse reguleerimine;
6.2.11. kaughalduse tugi;
6.2.12. käsurealt juhtimine üle turvakanali (SSH);
6.2.13. graafiline kasutajaliides.

[5] See on üks väheseid, mida ei ole veel suudetud lahti murda (2017.a.)
[6] Kolmanda generatsiooni tulemüürid, lisaks esimese ja teise põlvkonna tulemüüridele vaatab ka iga paketi asetust paketiseeria sees. Säilitatakse teave kõigist ühendustest, mis tulemüüri läbivad, ning on võimelised määrama, kas konkreetne pakett kujutab endast uue ühenduse algust, on osa praegusest ühendusest või on hoopis vigane pakett.

7. VÕRGULÜLITI

7.1. Kõige kiirem võrgulülitite-vaheline andmevahetus toimub üle pinu (*stackable*) ühenduste. Seega on kõige parem jõudluse ja pordi hinna suhe üldjuhul alati 24-port, seadmete paigaldamise püstraami paigaldatavatel ning täielikult hallatavatel gigabit kiirusega võrgulülititel. Soetamisel tuleb arvestada portide arvu 15-25% liiasusega. Seadmete töökindluse tõstmiseks tuleks eelistada ilma liikuvate osadeta (näiteks ventilaatorid) lüliteid. Püstraami paigaldatavad seadmed tagavad parema laiendatavuse tulevikus.

Soovituslik on 1 GB kiirusel töötav seade, mis toetab vajadusel 10 Mbit/s ja 100 Mbit/s ühendusi. Seade peab olema kaughallatav ning vähemalt layer 2 turvakontrolliga.

7.2. Soovituslikud nõuded võrgujaoturile:
7.2.1. 10/100/1000Base tugi kõikidel portidel. Tulevikus laienduse tagamiseks on vajalik vähemalt 2x SFP pordi olemasolu (ilma tootja lukustuseta, võimalik kolmandate osapoolte SFP moodulite kasutamine ilma piiranguteta);
7.2.2. avatud vormingus logimine ja ühilduvus enamlevinud haldusrakendustega
7.2.3. SNMP tugi;
7.2.4. portide peegeldamise funktsioon mitu-ühele;
7.2.5. pääsupunktide halduse võimekus (hankimisel defineerida hallatavate pääsupunktide arv) ja lõppseadmete rändluse (*roaming*) tugi;
7.2.6. QoS tugi: Voice VLAN ja Wireless multimeedia;
7.2.7. IEEE 802.1Q virtuaalsete kohtvõrkude (VLAN) tugi;
7.2.8. IEEE 802.1XPort-based Access Control & Guest VLAN tugi;
7.2.9. WPA2 Personal ja Enterprise versioonide tugi;
7.2.10. tasuta tarkvarauuendused kogu eluea vältel;
7.2.11. soovituslik eluaegne garantii;
7.2.12. Vajadusel 802.3af (PoE) või 802.3at (PoE+) tugi (ilma vajaduseta seda mitte lisada).

8. SERVERID

8.1. Serverlahenduses on soovituslik kasutada minimaalselt 2 füüsilist serverit ning nende peal töötavaid virtuaalservereid. Serverite riistvara peab olema toetatud operatsioonisüsteemi tootja poolt soovitatud nõuetele vastava virtualiseerimistarkvara kui ka operatsioonisüsteemidega. Serverite andmeside toimub läbi dubleeritud gigabitiste (või 10 GB) võrguseadmete. Riistvara peab olema varustatud spetsiaalsete kaughaldustarkvaraga, et tagada ligipääs tõrgete korral. Kogu serverite riistvara tuleb kaitsta puhvertoiteallikatega.

Rakenduste käitamine ilma virtualiseerimiskeskkonnata ei ole soovitatav ning seda võib kasutada ainult äärmisel vajadusel (otse füüsilisel serveril). Serverid peavad olema majutatud kas teenusepakkuja juures või KOV serveriruumis, mis vastab vähemalt ISKE turvaklassile L, kuid

mitte madalam, kui kõige kõrgema ISKE klassiga majutatav andmekogu. (vt https://www.ria.ee/public/ISKE/AndmekeskuseTurvanouded.pdf).

8.2. Soovituslikud minimaalsed nõuded serverile:
8.2.1. toetab virtualiseerimise lahendus VMware; Hyper-V jne;
8.2.2. serverite võimsus, mälud jne on sõltuvuses serveritele planeeritavate süsteemide ja rakenduste vajadusega;ning omavad komponentide laiendamis võimalust.
8.2.3. toide: vähemalt 2 toiteplokki koos modulaarse jahutusega;
8.2.4. toiteplokid vastavad toitepingele 220V, on vähemalt dubleeritud ning ühe toiteploki töö lakkamine ei põhjusta seadme väljalülitumist;
8.2.5. server peab võimaldama kaughaldust;
8.2.6. soetatavate serverite garantiiaeg on soovitatav võtta sama pikk kui on eeldatav serveri eluiga (keskmine serveri eluiga on 5 aastat). Kui serverid on soetatud projektipõhiselt, siis on kohustuslik tagada serveri eluiga vastavalt projekti finantseerimistingimustele.

9. ARVUTITÖÖKOHAD

9.1. Arvuti operatsioonisüsteem peab olema suuteline suhtlema KOV sisevõrgu domeenkontrolleriga[7].

9.2. Arvutitel peab olema kohtvõrgus äratamise võimekus (WOL).

9.3. Mobiilsete töökohtade puhul peab kasutama kõvaketta krüpteerimist.

9.4. Välistada tuleks operatsioonisüsteemide segakasutus[8].

9.5. Juhul kui kasutatakse Microsoft Exchange Serverit, siis on soovitatav kasutada Microsoft Office kontoripaketti, et kogu funktsionaalsus oleks kasutatav[9].

10. KASUTAJATE HALDUSTEENUS

[7] võrgu domeen on loogiliselt ühte kuuluv operatsioonisüsteemiga arvutite grupp, mis jagavad keskset andmebaasi. Jagatav andmebaas sisaldab domeeni kuuluvate kasutajate kontosid (igal kasutajal on unikaalne konto koos selle kontoga seotud õigustega) ja turvainformatsiooni domeenis olevate ressursside kohta. Näiteks Windows 7 Professional, Windows 10 Professional.

[8] Näiteks kui on Windowsi võrk, siis kõik op süsteemid on Windows 7 Pro, kui on Linuxi võrk, siis kõik op süsteemid on Ubuntu. Iga lisanduv op süsteem tõstab administratori töökoormust.

[9] Kalendrid, asutuse aadressraamat, ruumide ja seadmete broneering on kasutatav ainult Microsoft Outlooki ning veebipostkasti OWA kaudu.

10.1. Teenus võimaldab kasutajaid hallata ning vastavalt vajadusele nende õigusi piirata ja muuta eri infosüsteemide vahel (näiteks võrgukettad, ühiskalendrid jne).
10.2. Kasutajate halduses peab olema võimalik kirjeldada nime, kasutajanime, parooli, ametinimetust, isikukoodi, töökoha aadressi, e-posti aadressi.
10.3 Soovitatav on kasutada sisevõrgus olevates tarkvarades keskset sisselogimise teenust (*Single Sign-on*).

11. LÕPPSEADMETE HALDUS

KOV IKT taristu seadmeid peab olema võimalik hallata ühtsete reeglite järgi, sh uuendada tarkvara versioone, määrata rakenduste ligipääsu õigusi, eemaldada või lisada tarkvara, seirata IKT seadmete seisukorda ning pidada arvestust varade üle.

12. E-POSTI TEENUS

12.1. E-posti teenus peab võimaldama ametnikul kasutada kõiki grupitöö vahendite võimalusi info vahendamiseks, kohtumiste korraldamiseks ning ruumide ja seadmete broneerimiseks. E-kirjad peavad olema sünkroonis nii lokaalses arvutis olevas e-posti rakenduses, veebipõhises postkastis ning vajadusel ka nutiseadmes.
12.2. Soovituslikult võiks e-posti teenus sisaldada listide ja meiligruppide kasutamise võimalust ning sünkroniseeritud kalendrit, mida saavad näha kõik sama KOV ametnikud ning vajadusel ka KOV allasutused, kes kasutavad sama lahendust.
12.3. E-posti lahendus peab olema seotav keskse kasutajate halduse ja autoriseerimisteenusega.
12.4. E-posti teenus peab sisaldama ka viiruse- ja rämpsposti tõrjet.

13. VIIRUSETÕRJE

13.1. Viirusetõrje peab olema keskselt hallatav ning seiratav. Viirusetõrje peab olema rakendatud kohustuslikult kõigile KOV arvutitele ilma kasutajapoolse väljalülitamise võimaluseta.
13.2. Viirusetõrje peab olema rakendatud ka asutuse serveritele.
13.3. Viirusetõrje keskne haldus peab võimaldama kasutajate arvutite viirusetõrje tarkvara versiooni uuendamist.

14. VARUKOOPIA JA TAASTEPLAAN

14.1. Varukoopia tagab KOV-ile seadmerikke, seadme hävimise, viirusrünnaku või muu intsidendi järel andmete ja infosüsteemide taastamise võimaluse.

14.2. KOV peab välja töötama varundusplaani, kus on kirjeldatud, milliseid infosüsteeme varundatakse ning millise ajagraafiku alusel (päev/nädal/kuu jne).

14.3. KOV peab välja töötama taasteplaani kus on kirjeldatud üksikasjalik käitumisjuhend KOV-i infosüsteemi avarii puhuks eesmärgiga minimeerida kahjusid. Plaan koostatakse nii, et avarii

korral infosüsteemi kriitilise tähtsusega osade töövõime säiliks või taastuks võimalikult lühikese ajaga.

14.4. Varukoopia tarkvara peab võimaldama varundada nii füüsilisi kui virtuaalseid servereid sisevõrgus.

14.5. Andmete taastamise protseduur peab olema dokumenteeritud (taasteplaan) ning taastamine peab olema võimalik nii faili-, süsteemi- kui ka kasutajapõhiselt.

14.6. Vähemalt üks varukoopia kogu süsteemist (andmed, virtuaalserverid, rakendused jne) peab olema ka serveriruumist väljaspool (näiteks teeninduspunktis), et tagada andmete taastevõimalus serveriruumi seadmete hävimisel.

14.7. Varukoopia taasteproove tuleb läbi viia regulaarselt, soovituslikult kord aastas, et veenduda varukoopia töötamises.

15. PBX (VOIP)

VOIP teenus on mõistlik tellida välise teenusepakkuja käest ning ilma kohapealse VOIP jaamata. Telefoniside peab toimuma üle IP võrgu ning soovituslikult tuleks tagada võimalus kasutada lauatelefoni numbrit nutiseadmes (SIP protokoll).

16. FAILIHALDUS

16.1. Lisaks asutuse dokumendi- ja infohaldustarkvaras menetluses olevale infole on vaja hallata asutusesiseselt kasutajate tööks vajalikke faile.

16.3. Kasutajatele peab olema loodud turvaline keskkond tööfailide salvestamiseks ja hoidmiseks kas võrguketaste näol või pilvekeskkonnas.

16.4. Soovitatav on sisse lülitada failiversiooni haldus, et kasutaja saaks vajadusel ise faile taastada eelmistesse versioonidesse.

17. KOV IKT VÕRGU DOKUMENTATSIOON:

17.1. infosüsteemide kasutamise kord;
17.2. infoturbepoliitika;
17.3. Taasteplaan
17.4. Võrgujoonised
17.5. ISKE dokumentatsioon