

SOOVITUSED IT-TEENUSTE KORRALDAMISEKS

Üldhariduskoolide digitaristu
kaasajastamine

SISUKORD

OLULISEMAD MÕISTED JA LÜHENDID	3
SISSEJUHATUS	5
1. TEENUSTE KOOSVÕIMEST	7
2. KLIENDISPETSIIFILISED IT-TEENUSED	10
2.1. Õppeinfosüsteem	10
2.2. Õppematerjalide hoidla.....	10
2.3. Õpikeskkonnad	11
2.4. Haridusasutuse koduleht ja <i>intranet</i>	12
2.5. Dokumendihaldussüsteem	12
3. UNIVERSAALSED IT-TEENUSED	13
3.1. Arvutitöökoha teenus	13
3.1.1. Printimine.....	15
3.1.2. Pahavaratõrje	15
3.2. Kasutajate isikutuvastus ja -õiguste haldamine	15
3.3. E-post, kalendri, postiloendite ja grupitöö lahendus	16
3.4. Failide hoidmine	17
3.5. Telefonside.....	18
3.6. Kaugligipääs.....	18
3.7. Videokonverents	18
3.8. Infoturve.....	19
4. TARISTU TEENUSED.....	21
4.1. Andmete ja serverite majutamine	21
4.1.1. Varundamine	22
4.2. Andmeside (kohtvõrgud ja wifi).....	22
4.2.1. Võrguseadmete haldamine	23

OLULISEMAD MÕISTED JA LÜHENDID

- 1) **EHIS** – Eesti Hariduse Infosüsteem
- 2) **EKIS** – Eesti Koolide Infosüsteem
- 3) **Haridusasutus** – eelkõige koolieelsed lasteasutused, põhikoolid ja gümnaasiumid, kutseõppeasutused, rakenduskõrgkoolid, ülikoolid, huvikoolid ning täienduskoolitusasutused, samuti neid teenindavad teadus- ja metoodikaasutused.
- 4) **Hariduse infosüsteem** – haridusasutustes kasutatavate infosüsteemi komponentide kogum, mille abil peetakse haridusarvestust, korraldatakse ja koordineeritakse õppetöö protsesse ning hallatakse haridusasutuste igapäevast tööd.
- 5) **HITSA** – Hariduse Infotehnoloogia Sihtasutus
- 6) **HTM** – Haridus- ja Teadusministeerium
- 7) **Infoturve** (ehk andmekaitse) on andmete kolme põhiomaduse – tervikluse, käideldavuse ja konfidentsiaalsuse tagamine, kus:
 - 7.1. **käideldavus** tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
 - 7.2. **terviklus** tähendab, et info pärineb usaldusväärsest allikast ning seda ei ole volitamata muudetud ega kustutatud;
 - 7.3. **konfidentsiaalsus** tähendab, et informatsioon on kättesaadav vaid volitatud isikutele.
- 8) **IKT** – info- ja kommunikatsioonitehnoloogia; kasutusel ka sünonüümina IT ehk infotehnoloogia.
- 9) **Kasutaja** (kasutusel ka lõppkasutaja, -tarbija) – isik, kes kasutab IT-teenust pidevalt (nt õppija, õpetaja, administratiivtöötaja); eristatakse kasutajaid ja kliente, mitte iga klient ei kasuta otseselt IT-teenust.
- 10) **Klient** on kaupade või teenuste ostja/saaja; IT-teenuse osutaja klient on isik või grupp (näiteks haridusasutuse esindaja), kes määrab ja lepib kokku nõuded teenusele.
- 11) **Teenus** on väärtuse pakkumine klientidele nende soovitud lõpptulemuste saavutamiseks. **IT-teenus** kasutab infotehnoloogiat ja toetab haridusasutuse tööprotsesse. IT-teenused jagunevad põhimõtteliselt kolmeks: a) kliendispetsiifilised IT-teenused, b) universaalsed IT-teenused ja c) taristu (ehk infrastruktuuri) teenused.
- 12) **Teenuseosutaja** (sünonüümina ka teenusepakkuja) on organisatsioon, mis osutab teenuseid kliendile; kui IT-teenuseid ostetakse sisse, kasutatakse mõistet **väline teenusepakkuja**.
- 13) **Teenuslepe** (*Service Level Agreement, SLA*) on kirjalik lepe IT-teenuse osutaja ja kliendi ehk haridusasutuse esindaja vahel. See kirjeldab IT-teenuse, dokumenteerib teenustaseme nõuded (minimaalselt süsteemi käideldavusele, andmete konfidentsiaalsusele ja terviklusele) ja spetsifitseerib poolte vastutused.
- 14) **Vabavara** (*free software*) on tarkvara, mida kasutajal on õigus muuta ja levitada.
- 15) **Tootjalukustus**¹ (*vendor lock-in*) on kliendi sõltuvus tootja pakutavatest toodetest või teenustest tehnoloogilise salastatuse kaudu (suletud, firmasisesed ja -omased, mõnikord ka patenteeritud standardid, tehnilised normid, spetsifikatsioonid). Sõltuvust ilmestab asjaolu, et mõne teise tootja vastu välja vahetamisega kaasneksid märkimisväärsed

¹ <https://wiki.pingviin.org/Tootjalukustus>

kulud. Lukustuskulud, mis tekitavad turgudele sisenemisbarjääre, võivad omakorda põhjustada umbusaldust monopolide suhtes.

- 16) **Varundamine** (*back up*) on andmetest varukoopiate tegemine, et võimaldada andmete hilisem taastamine.



SISSEJUHATUS

Ulatuslik info- ja kommunikatsioonitehnoloogia (IKT) areng on vastastikku mõjutanud organisatsioonide toimimist. Kui ühelt poolt võimaldab tehnoloogia senisest kvaliteetsemat ja kiiremat teenuse osutamist, siis teiselt poolt sunnib järjest keerulisemate süsteemide kasutamine pöörama kasvavat tähelepanu informatsiooni, andmete ja kaasnevate riskide juhtimisele.

Ka hariduse valdkonnas kasutatakse järjest enam IT-lahendusi, mis aitavad kaasa õppetöö tulemuslikkusele ja haridusasutuste toimimisele. IKT-põhiste õppevaralahenduste kasutamine ja üldise digivõimekuse tõstmine seab omad nõuded nii personalile kui ka vajalikule tarkvarale ja taristule, muu hulgas arvutitöökohtadele ja esitlustehnikale (ehk seadmetele).

Käesolev dokument avab lugejale (eelkõige üldhariduskoolide juhtidele ja koolipidajatele) IT-teenuste sisu ja hõlmab soovitusi haridusasutustele IT-teenuste juhtimise korraldamiseks, sh IT-teenuste juhtimise parimat praktikat, viiteid vajalikele rollidele koos ülesannetega, IT-teenuste jagunemist ja sisu kirjeldusi ning nõudeid, millele haridusasutuste IT-teenused peavad minimaalselt vastama. Põhjalikuma huvi korral on dokument on varustatud mitmete viidetega.

Arvestades haridusasutuste mitmekesisust² nii funktsioonide kui ka suuruse poolest, ei eelda see dokument, et kõik kirjeldatud teenused on igal pool kasutusele võetud täies mahus. Teenuste valikul, arendamisel ja haldamisel tuleks lähtuda maksumuse, ühishuvide ja andmekaitse reeglite täitmise kaalutlustest:

- 1) analüüsida erinevaid lahendusi ja võrrelda nende **maksumust** (vabavaralised vs. litsentseeritud lahendused; teha ise vs. osta sisse; omada servereid vs. kasutada pilveteenuseid jne) ning teha teadlik valik, püüdes vältida tootjalukustust ja sellega kaasnevaid kulusid tulevikus;
- 2) aru saada haridusasutuse arenguvisionist ja riigi arendusprioriteetidest, eristada **ühishuve** üksikute vajadustest ning olulist ebaolulisest, st lahendus, mis on kasu(m)likum äriettevõtetele, ei ole üldjuhul haridusasutustele ja riigile tervikuna jätkusuutlik ning tekitab ebavõrdsust;
- 3) arvestada **andmekaitse reeglitega** (isikuandmete töötlemine ja kaitse, andmete säilimise tagamine jne) ja teiste Eesti kehtivate seaduste ja normidega (koosvõime raamistik³);
- 4) haridus, sh IKT-ga seonduv, peab olema kättesaadav kõikidele võrdsetel alustel ehk jäädavalt tasuta. IKT õpetamisega ei tohi luua varanduslikku ebavõrdsust ega anda maksumaksja raha kulul eelist äriettevõtetele monopolide soodustamisega. Erinevate tarkvara platvormide ja programmide õpetamine ja oskamine on kindlasti oluline, ent aluseks olev süsteem peab olema kõikidele võrdsetel alustel ehk jäädavalt tasuta

² Ülevaade Eesti üldhariduskoolide digitaristust

http://www.innovatsioonikeskus.ee/sites/default/files/tekstifailid/digitaristu_ylevaade_nov2014.pdf
(Detsember 2014)

³ <https://www.mkm.ee/et/riigi-infosusteemi-koosvoime-raamistik>

kättesaadav, st et vabataarkvara abil on võimalik IKT teadmised täies mahus õpetada kõikidel haridustasemetel⁴.

Lõplik vajadus ja IT-teenuste liigitus sõltub konkreetsest haridusasutusest ja tema võimalustest, ent unustamata seejuures peamist: IT on tõhusama õppetöö abivahend, mis aitab tagada haridusasutuse tööd, mitte asi iseeneses. Samas on tegemist kiirelt muutuva valdkonnaga, kus pidev areng on vältimatu. Seega on koolijuhi ja/või -pidaja ülesanne määrata selge vastutus ja volitus haridusasutuses IT-küsimustega tegelemiseks.

Eelnevalt on haridusasutuste tehnoloogiavaldkonna juhtimise toetamiseks loodud kogumik „IT juhtimise head tavad koolis“ (detsember 2014), mis katab IT-vajaduste kirjeldamise, IT-arengu juhtimise, IT-meeskonna rollide ja vastutuse, taristu loomise ja haldamise ning kooli IT-turvalisuse teemad ja annab ülevaate olulisematest seadustest, juhenditest ja kordadest.

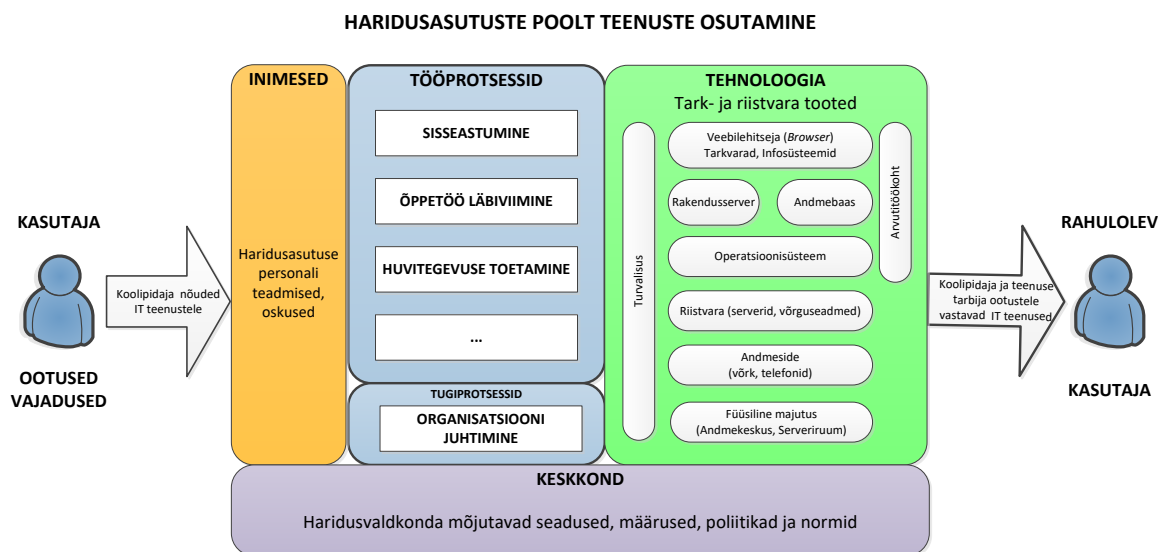
Arvestades, et teenuste väärtuslikkus lõpptarbijale sõltub haridusasutuse ja IT koostööst, on kõik huvigrupid oodatud esitama ettepanekuid haridusvaldkonna IT-teenuste parendamiseks ja aktiivselt osalema teenuste arendusprojektides. Kui teil tekib siinsete soovitustega seoses küsimusi, palun pöörduge info@hitsa.ee.

⁴ <http://goo.gl/JAUsfC>

1. TEENUSTE KOOSVÕIMEST

Teenus on väärtuse pakkumine klientidele nende soovitud lõpptulemuste saavutamiseks. **IT-teenus** kasutab infotehnoloogiat ja peab toetama (haridus-)asutuse tööprotsesse.

Kuna teenused koosnevad **kolmest komponendist**: inimestest, protsessidest ja tehnoloogiast, peavad lõpptarbijale (õpilane, õpetaja, lapsevanem, koolipidaja) väärtuse loomiseks kõik osad olema läbimõeldud, toimima kooskõlas ja kõikidele võrdsetel alustel. Ärihuvidest, tootjalukustusest vmt lähtuvad kulutused ei ole põhjendatud. Seega peavad haridusasutuse personalil olema piisavad oskused ja kogemused, seda toetav optimaalne töökorraldus ning kuluefektiivne ja tootjalukustusest vaba tehnoloogia ja lahenduste valik, unustamata keskkonnast tulenevaid piiranguid (vt Joonis 1).



Joonis 1: komponendid, millest oleneb haridusteenuse osutamise kvaliteet ja tulemuslikkus.

IT-teenused jagunevad põhimõtteliselt kolmeks:

- 1) **Kliendispetiifilised IT-teenused** on seotud haridusasutuse põhi- ja tugiprotsesside toimimisega; eelkõige on tegemist haridusasutusele iseloomulike tööprotsessidega (näiteks õppetöö korraldamine, huvitegevuse pakkumine, asjaajamine, ressursside haldamine jne), mis kas osaliselt või täielikult on automatiseeritud ehk toetatud mõne IT-lahendusega;
- 2) **Universaalseid IT-teenuseid** kasutatakse tavapärase tööde toetamiseks (näiteks e-posti saatmine, printimine, telefonside jne);
- 3) **Taristu** (ehk infrastruktuuri) **teenused** on vajalikud teiste IT-teenuste toimimiseks (näiteks andmete ja serverite majutus (sh piisav jahutus, elekter, ruumid), varundamine jne).

Lisaks peab meeles pidama, et õppekorralduse ja IT koosvõimest saame rääkida üksnes juhul, kui IT-teenused on samaaegselt nii **eesmärgipärased** kui ka **kasutatavad** ehk toetavad haridusasutuse tegevusi ja on kättesaadavad kokkulepitud ajal. Iga IT-teenuse eesmärgipärasus (ehk sisu) ja kasutatavus (nõuded) tuleb kokku leppida kliendi (näiteks

koolipidaja, koolijuht, arendusjuht) ning (välise) teenusepakkuja (näiteks IT-juht, firma esindaja) vahel **teenusleppe vormis**.

Teenuslepe (*Service Level Agreement, SLA*; ka teenustasemelepe) on kirjalik lepe IT-teenuse osutaja ja kliendi ehk haridusasutuse esindaja vahel. See kirjeldab IT-teenuse olemuse, dokumenteerib teenustaseme nõuded ja spetsifitseerib poolte vastutused.

Lühidalt kajastatakse teenusleppes teenuse põhifunktsionaalsuse lühikirjeldus (ehk selle otstarve), selle mittetöötamise mõju tööprotsessile ja seotus teiste teenustega (ehk andmevahetus teiste süsteemidega) ning kasutajad (rollid ja arv). Samuti fikseeritakse teenuse käideldavus (tööaeg), lubatud katkestuste aeg, nõuded andmete käideldavusele, terviklusele, salastatusele ja varundamisele ning tingimused katkestustele, reageerimis- ja lahendamisaegadele, sidekanalile ja selle reaktsiooniajale ning -keelele. Väga oluline osa operatiivseks infovahetamiseks on kirja panna seotud poolte kontaktid. IT-teenuste ajakohasuse tagamiseks on tsentraalseteks tark- ja riistvarauuendusteks mõistlik kokku leppida hooldusaeg (näiteks kord nädalas).

Kokkulepitud IT-teenuse nõuded on oluline sisend kasutajatoe korraldamiseks ehk hilisemate kasutaja pöördumise lahendamiseks ja seeläbi teenusega kõrge rahulolu tagamiseks. Vastavalt kokku lepitud reageerimis- ja lahendamisaegadele on kasutajatoe ülesanne taastada teenuse toimimine nii kiiresti kui võimalik. Teenuse parendamiseks tuleb perioodiliselt kasutajate pöördumisi analüüsida, vajadusel alatatada ja ellu viia muudatusi teenuse kvaliteedi järkjärguliseks tõstmiseks.

Teenusleppeid on mõistlik üle vaadata ja uuendada vähemalt kord aastas. Kõik tarbitavad ja pakutavad IT-teenused peavad olema ajakohased nii sisult, versioonilt kui ka platvormilt ning kehtiva hoolduslepinguga. Selleks et garanteerida järjepidev ja otstarbekas IT-teenuse hooldus- ja arendusvõimekus, on sageli mõistlikum kasutada (välise teenusepakkuja) standardseid lahendusi rätseplahenduste ise arendamise asemel.

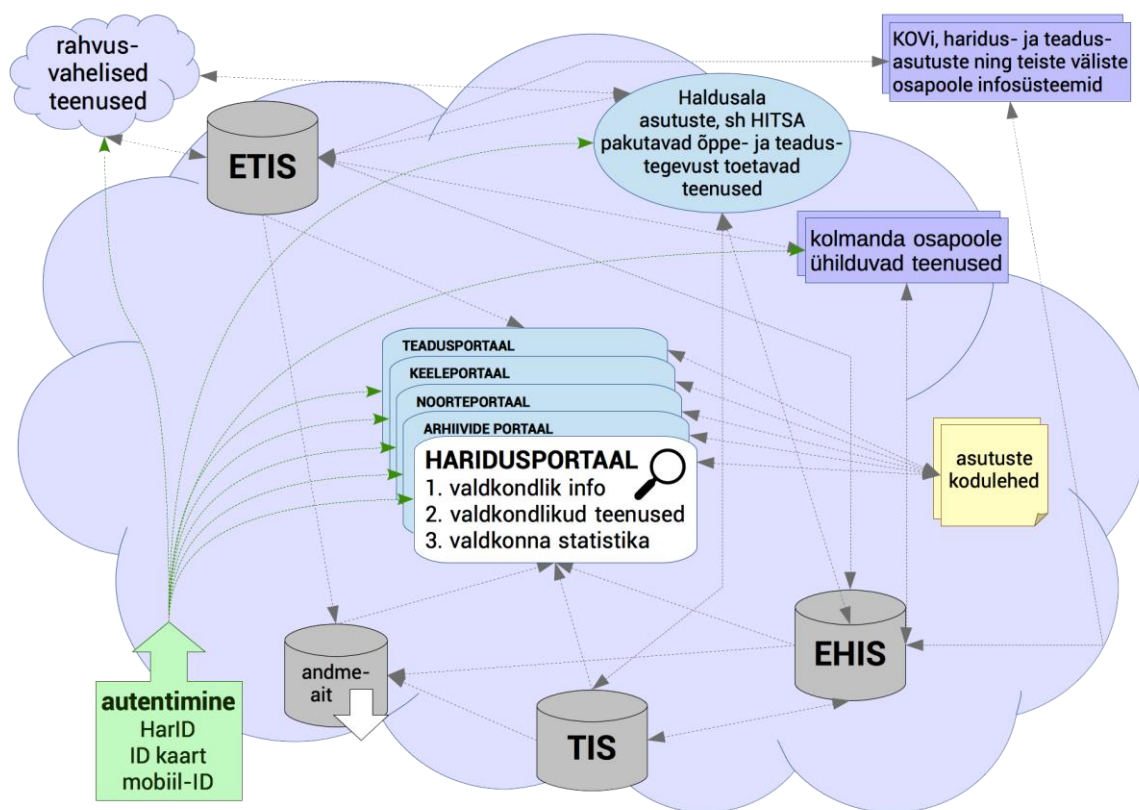
Teenuste omavahelisi sõltuvusi ja toimimist käsitletakse koosvõimena. **Hariduse infosüsteemi** (ehk kõikide haridusvaldkonna IT-lahenduste) **koosvõime** eesmärk on tagada nii haridusasutuses kasutatavate infosüsteemide kui ka riigi infosüsteemi kuuluvate andmekogude omavaheline automatiseeritud andmevahetus. Pikemalt saab hariduse infosüsteemi koosvõimest lugeda [siit](#). Lisaks kehtib Majandus ja Kommunikatsiooniministeeriumi (MKM) loodud koosvõime raamistik⁵, mis mh reguleerib elektrooniliste dokumentide failivorminguid. Kasutama peab avatud ja vabadel standarditel põhinevaid andmevorminguid ning vältima tootjalukustust ning tasulist tarkvara, vaid siis on loodud eeldused riigi infosüsteemide koosvõimeks.

Haridusasutused on oma otsustes vabad valima endale sobivaid infosüsteeme ja teenuseid, ent seejuures tuleb silmas pidada, et eelistama peaks:

- avatud infosüsteeme, mis pakuvad andmevahetuse võimalust teiste süsteemidega standardlahendusena (vt ka MKM koosvõime raamistik);

⁵ <https://www.mkm.ee/et/riigi-infosusteemi-koosvoime-raamistik>

- üldjuhul teenusena pakutavaid lahendusi haldamis- ja majutuskulude vähendamiseks;
- kasutaja (õppija ja õpetaja) vaatest loodud teenuseid ja infosüsteeme.



Joonis 3: Hariduspilv ja selle komponendid;

Lühendid: ETIS = Eesti teadusinfosüsteem; TIS = testide infosüsteem (praegune EIS ehk eksamite infosüsteem); EHIS = Eesti hariduse infosüsteem

Hariduse infosüsteemi oodatavat koosvõimet ja omavahelisi seoseid illustreerib pilt (ehk hariduspilv). Hariduspilve kontseptsioon näeb tulevikus ette digitaalse hariduskeskkonna loomist, mille eesmärk on parandada hariduse osapoolte suhtlust ning koostööd. Hariduspilv võimaldab õpilastele, õpetajatele ja teistele osapooltele ligipääsu haridusvaldkonna andmebaasidele ja infosüsteemidele, mis toetavad õpet ja haldustegevusi koolides. Pilv on ligipääsetav kõigile võrdsetel alustel.

2. KLIENDISPETSIIFILISED IT-TEENUSED

Kliendispetsiifilised IT-teenused on seotud haridusasutuse põhiprotsessiga (ehk õppetööga), ent võivad erineda ja sõltuda iga asutuse eripärast. Reeglina on kliendispetsiifiliste teenuste lõpptarbijateks õpilased, õpetajad, lapsevanemad, koolipidaja. Levinumatest haridusvaldkonna kliendispetsiifilistest teenustest annab ülevaate järgnev peatükk.

2.1. Õppeinfosüsteem

Eestis kasutatakse mitut erinevat õppeinfosüsteemi: ülikoolidel oma lahendus, rakenduskõrgkoolidel HITSA pakutav õppeinfosüsteem (ÕIS), kutsekoolidel Siseveeb, üldhariduskoolidel e-kool või Stuudium.

Õppeinfosüsteem peab toetama haridusasutuse põhiprotsessi ning võimaldama minimaalselt:

- 1) õppetöö korraldamiseks vajalike andmete haldamist ja õppetöö planeerimist: õppekavade ja õppeainete andmete haldamine, õppejõudude kohta õppetöö korraldamiseks vajalike andmete haldamine, koormuste ja tunnijaotuse planeerimine, tunniplaani haldamine;
- 2) õppurite haldamist: uute õppurite lisamine, õppurite staatuste muutmine (näiteks akadeemilised puhkused), õppeasutuse lõpetamine või õppeasutusest väljaarvamine;
- 3) õppetöö jooksvat korraldamist: õppurite registreerimine õppeainetele, õppepraktika tegemise korraldamine, lõputööde tegemise korraldamine, õppetulemuste (hinnete) sisestamine, õppurite õppekava täidetuse jälgimine.

Väiksema administratiivse koormuse ning parema andmete kvaliteedi tagamiseks peab õppeinfosüsteem olema koosvõimeline teiste riigi infosüsteemidega (nt Töötajate Register, Riigitöötaja Iseteenindusportaal, Eesti Hariduse Infosüsteem (EHIS), Eesti Koolide Infosüsteem (EKIS) jne) ning võimaldama keskse autoriseerimislahenduse kasutamist (vt isikutuvastusteenus) või liidestust autoriseerimislahendusega HarID kaudu. HTMi IT-arenduse põhimõtted näevad ette koosvõimelist õppetööd toetava õppeinfosüsteemi kasutuselevõtmist.

2.2. Õppematerjalide hoidla

Õppematerjalide hoidla (*kasutatakse ka repositooriumi ja failihoidla nimetust*) on tehniline keskkond elektroonsete dokumentide ehk failide säilitamiseks ja töötlemiseks. Mõistel failihoidla on siin kaks tähendust: a) õppematerjalide hoidla ja b) klassikaline failihoidla isiklike töödokumentide haldamiseks töökoha arvutis ja/või pilveteenuses (vt peatükk failide haldamine). Õppematerjalide hoidla peab kasutaja seadmest ja kasutatavast tarkvarast olenemata võimaldama õppevara otsimist, kasutamist ja salvestamist. Digitaalse õppevara hulka kuuluvad e-õpikud, e-töövihikud, e-õpetajaraamatud, veebipõhised hindamisvahendid, aga ka üksikobjektid, mida õppetöös on võimalik kasutada.

Elektroonsete õppematerjalide loomisel tuleks lähtuda MKMi koosvõime raamistikus sätestatud avatud ja vabadest failivormingutest. Kui dokumendid luuakse pilveteenuses vabatarkvara abil, muutuvad need kohe kättesaadavaks ja kasutatavaks ja ühtlasi on tagatud andmetest ka varukoopia ja võrgupõhise koostöö võimalused. Suletud ja patenteeritud failivormingutes e-materjalide loomine tekitab probleeme ühilduvusega ning haridusasutustele ja koolipidajatele lisakulutusi. Reaalse digitaalse koosvõime loomiseks saab iga haridusasutus propageerida avatud standarditele põhinevate materjalide loomist. HTM tellib Euroopa Sotsiaalfondi (ESF) Digipöörde programmis üldhariduse ja kutsehariduse astmetele uusi digitaalseid õppematerjale.

HITSA osutab digitaalsete õppematerjalide jagamise teenust, mida pakutakse infotehnoloogiliste lahenduste abil. See võimaldab õppematerjalide avaldamist ja levitamist, tagades avaldatud materjalide säilimise ning kättesaadavuse. Praegusteks lahendusteks on: Koolielu Waramu, e-õppe repositoorium, Moodle, aga metaandmete tasemel ka e-Koolikott.

e-Koolikott on digitaalse õppevara portaal, mis koondab õppekava alusel märksõnastatult digitaalse õppevara ühte veebikeskkonda, eelkõige sisaldades õppevara alus-, üld- ja edaspidi ka kutseharidusele. e-Koolikoti peamine eesmärk on võimaldada ligipääs digitaalsele õppevarale ühest kohast – kasutaja ei pea enam otsima materjale erinevatest portaalidest. Märksõnastamiseks on loodud riiklik metaandmete süsteem, mis põhineb õppekavade ülesehitusel, tunnustel, teemadel jmt. Õppevara on võimalik otsida üldpädevuste, läbivate teemade, klassi, haridustaseme, ainekava teemade ning õppevara liigi järgi. Samuti saab otsida selle järgi, kas õppevara on tasuline või tasuta, ja kasutada teisi täpsustavaid kriteeriume.

2.3. Õpikeskkonnad

Õpikeskkond (*Learning Management System, LMS*) on tarkvaraline lahendus õppetöö ja dokumentide haldamiseks, aruandluseks ning e-õppe programmide pakkumiseks. Neist tuntumad on Eestis laialdaselt kasutatav Moodle ning välismaalt Udemy, Eliademy, edX ja Coursera. Rohkem lahendusi leiab [siit](#). Õpikeskkond peaks olema võimeline vahetama andmeid teiste hariduse infosüsteemidega (näiteks e-päevik, õppeinfosüsteem, EHIS, e-Koolikott jt) ja võimalusel olema kasutajale kättesaadav ka pärast haridusasutuse lõpetamist, võimaldamaks oma kogu haridustee hoiustamist ja haldamist (*Personal Learning Environment*).

HITSA pakub e-kursuste pidamiseks Moodle'it. Õpikeskkond Moodle hõlmab erinevaid e-õppe vahendeid ja tegevusi, mida saab e-kursusel kasutada (õppematerjalide esitamise võimalused, testid, ülesanded, foorumid jpm). Õpetajale loob see võimaluse õppetegevuse läbiviimiseks ja õpilasele e-vormis õppimiseks. Teenus on tasuta Eesti üldhariduskoolidele ja e-Ülikooli ning e-Kutsekooli konsortsiumi liikmeskoolidele, kõigile teistele pakutakse teenust [hinnakirja](#) alusel, olenevalt e-kursuse kasutajate arvust.

2.4. Haridusasutuse koduleht ja intranet

Koolide praeguseid kodulehti iseloomustab ebaühtlus ja mitmekesisus nii olemuselt (sisult ja disainilt) kui ka tehniliselt. Veebilehtede ja platvormide paljus, aga ka vanus muudab nende turvalisuse tagamise, arendamise ja sisuloome ressursimahukaks. HITSA töötab haridusasutustele kasutamiseks 2017. a jooksul välja kesksel sisuhaldustarkvaral ja ühtsetel halduspõhimõtetele tugineva veebimajutuse ja -platvormiteenuse, mis on koosvõimeline teiste infosüsteemidega ja vastab haridusasutuste üldistele kodulehtedele esitatavatele vajadustele.

Intranet on asutusesisene suhtlusvahend, mis võimaldab suhtlemist ja vajaliku info vahetamist kasutajate vahel. Tavapäraselt sisaldab *intranet* asutuse sisemiseks toimimiseks vajalikku informatsiooni, dokumente, uudisvoogu, olles integreeritud teiste IT-lahendustega (näiteks videokonverentsiga).

2.5. Dokumendihaldussüsteem

Haridusasutuse toimimise lahutamatuks osaks on dokumendihaldus, asjaajamine ja arhiivindus, mis tihti on seotud mõne IT-lahendusega. Üks võimalustest on kõigile haridusasutustele avatud Eesti koolide haldamise infosüsteem (EKIS), mis on registreeritud Eesti Hariduse Infosüsteemis (EHIS).

EKIS on arendatud haridusasutuse vajadusi ja eripära silmas pidades. See sisaldab dokumendihalduse, finantsarvestuse, personalihalduse, varahalduse, raamatukogu, kooli töö, *intraneti* ja kommunikatsioonimoduleid ning on liidestatud dokumendivahetuskeskkonna (DVK) ja avaliku veebiga. Tänu sellele võimaldab EKIS koolidel täita kõiki dokumendihaldusega seotud nõudeid.

Tegemist on tänapäevase veebipõhise lahendusega, mis on teostatud digitaalse asjaajamise nõudeid, vajadusi ja andmete turvalisust silmas pidades. Veebipõhisest lahendusest tulenevalt ei vaja see IT-lahendus lisatarkvara paigaldamist kasutaja masinasse ning võimaldab seda kasutada turvaliselt kõikjalt, kus on internetiligipääs: kontor, kodu, internetikohvik. EKIS baseerub vabavaralistel komponentidel ega nõua seetõttu operatsioonisüsteemist, andmebaasimootorist vms tulenevaid lisalitsentside tasusid.

HTMi eestvedamisel konsolideeritakse ja ühtlustatakse riigikoolides (2017.–2018. a jooksul) dokumendihaldusvaldkond. Olenemata, missugust IT-lahendust asjaajamise hõlbustamiseks kasutatakse, peab meele pidama andmete töötlemise ja infoturbe reegleid (vt peatükk Infoturbe).

3. UNIVERSAALSED IT-TEENUSED

Universaalsed IT-teenused (näiteks arvutitöökoht, e-post, kiirsuhtlus, printimine (või selle asemel pilvepõhiste lahenduste kasutamine ja võrgupõhise koostöö soodustamine), failide haldamine, telefonside jne) on sisult üldjuhul standardsed, olenemata teenuse tarbijast ning vajalikud haridusasutuse tööprotsesside toetamiseks. Tõsi, erinevatele kasutajagruppidele (näiteks õpilasele või õpetajale) võib ette näha teenuse osalist (erinevate funktsionaalsuste) kasutamist või erinevaid kasutustingimusi (teenuse tasemeid), mis kõik lepitakse kokku (välise) teenusepakkujaga teenusleppes (vt peatükist Teenuste koosvõime). Järgnev annab ülevaate levinumatest universaalasest IT-teenustest, mis on vajalikud tööprotsesside toetamiseks.

3.1. Arvutitöökoha teenus

Nii infoühiskonna hüvede tarbimiseks kui ka klassiruumis õpetamiseks on vaja arvutitöökohta, mis üldjuhul koosneb riistvarast (laua- või sülearvuti, monitor, klaviatuur ja hiir), tarkvarast (näiteks (pilvepõhine) tarkvara (MSOffice või Libreoffice), kiirsuhtlustarkvara (Skype)) ja toetavatest teenustest (näiteks e-posti- ja kalendriteenus, printimine, kaugligipääs, failide haldamine). Kasutajale võimaldatakse seadmed ning tarkvara vastavalt töökohta profiilile ja haridusasutuse või koolipidaja võimalustele. Klassiruumis asuva õpetaja arvutitöökohta standardvarustuse hulka peaks kuuluma kõlarid ja projektor vm esitlusseade. Mobiilse töövahendi komplekti koostamisel tuleb lähtuda õpetaja tööspetsiifikast ja õppetöö protsessidest, mis võivad õppeaineti erineda. Mobiilne seade on oluline neile õpetajatele, kes annavad tunde õppeasutuse eri ruumides ja vajavad mobiilset töövahendit tööülesannete täitmiseks ka väljaspool kooli. Ruumid, mida kasutab mitu õpetajat, peavad olema varustatud nii, et iga õpetaja saaks tundi anda oma mobiilse seadmega. Koolimaja ruumide tehnoloogiaga varustamisel tuleb jälgida ning vajadusel arendada ka muu vajalik infrastruktuur (trepid, lift, juhtmega ja juhtmevaba võrk, elektriühendused jne), et see toetaks mobiilsete seadmete kasutamist. Taristu arendamisel on oluline tagada turvalisus, et kooli arvutivõrk, sellega seotud tehnoloogia ja andmed oleks kaitstud võimalike rünnakute või tehniliste rikete eest (nt elektrikatkestus, vargus, vandalism, volitamata juurdepääs jne). Kindlasti tuleb panustada täienduskoolitusse töötajate turvateadlikkuse tõstmiseks.

Õppetööga seotud andmed peavad olema lihtsalt ja kiirelt taastatavad – andmed tuleb varundada turvalises keskkonnas ja turvalise ühenduse kaudu. Mobiilne seade peab olema kaitstud pääsukoodidega ning tähtsad ja konfidentsiaalsed andmed tuleb hoida turvalises serveris või teenuses, millele ligipääsuks mobiilse seadmega tuleb kasutada turvalist ühendust kas virtuaalset privaativõrku (*Virtual Private Network, VPN*) või krüpteeritud (*Hypertext Transfer Protocol Secure, HTTPS*) ühendust. Teistele kasutajatele tuleb seadme kasutamiseks luua eraldi konto, mis tähendab, et õpetajast erinev kasutaja (nt õppija) saab seadme kasutamiseks eraldi kasutajanime ja parooli. VPN-lahenduse puudumisel tuleb kasutada turvalisi, krüpteeritud ühendust kasutavaid õpikeskkondi. Detailsemad soovitusel

ja kaalutlused mobiilse ja statsionaarse töökohale koolide digivõimekuse tõstmiseks leiab siit.

Kasutajate lõppseadmete (kõik asutuse väljastatud seadmed, hoolimata operatsioonisüsteemist) **haldamine** on soovitatav korraldada keskse halduslahenduse kaudu (näiteks *MS System Center Configuration Manager (SCCM)*, *MS Intune*, *Desktop Central* vmt). Keskne lahendus võimaldab operatiivselt koordineerida nii üksikuid (kõikide levinud operatsioonisüsteemide ulatuses) kui ka erinevate gruppide lõppseadmeid, määrata õigusi ja paigaldada või eemaldada tarkvarasid, viia ellu keskseid massmuudatusi, kasutada ühtset kaugligipääsu lahendust, automatiseerida IT-varade arvestust, lahendada kasutajate pöördumisi jmt. Eesmärk on viia lõppseadmete haldamise korral füüsilise sekkumise vajadus (kohapealne tegevus) miinimumini (kuni kaks juhtumit kümnest).

Arvutitöökoha teenuse kasutamise vältimatuks osaks on **andmeside ehk arvutivõrguteenus**, mille nõuetest pikemalt saab lugeda siit (ja peatükist Andmeside).

Arvestades arvutitöökoha ja andmesideteenuste olulisust kõikide teiste kliendispetsiifiliste- ja universaalsete IT-teenuste kasutamisel, tuleb kindlasti (välise) teenusepakkujaga kokku leppida teenuste tingimustes, sh kasutaja pöördumiste lahendamises (vt teenuslepe peatükist Teenuste koosvõimest). Üldjuhul saab arvutitöökohta ja andmeside teenuseid haridusasutuses kasutada tööpäeviti tööajal, ent arvutivõrku võib (osaliselt) sulgeda rikete ennetamiseks, avastamiseks ja kõrvaldamiseks, samuti teenuste hooldustöödeks.

Haridusasutuste töökorralduse ja õppetegevuse lahutamatuks osaks on **arvutiklasside ja esitlustehnika haldamine** (videoprojektoritest interaktiivsete tahvliteni). Arvutiklassis on soovitatav ja majanduslikult efektiivsem kasutada statsionaarseid seadmeid ehk kindla asukohaga lauaarvuteid. Arvutiklassi lauaarvuti komplektide puhul tuleb lähtuda õppetegevuse vajadustest ning komplektide hankimisel arvestada õpetatava tarkvara nõudmistest riistvarale. Ühe võimalusena soovitame kaaluda kõik ühes (*all-in-one*) tüüpi arvutit). Esitlustehnika valik sõltub ruumi suuruselt, esitlusvahendite arvust ja kasutusotstarbest. Populaarsust kogub videosalvestussüsteemide kasutamine õppetöös. Näiteks kõrgkoolides salvestatakse erialaseid loenguid, mida saab vaadata vastavalt seadistustele kas reaalajas või hiljem järelevaatamisena videokogust. Analoogselt saab veebikeskkonnas edastada mõne olulise sündmuse videosalvestusi, näiteks õppeaasta ava- või lõpuaktuse videopilti. Katkematu õppeprotsessi tagamiseks on mõistlik ette näha **varutehnika**, mida saab kasutusse võtta, kui mõni ese (näiteks arvuti, projektor) on saadetud remonti. Tasulise (sh suletud ja patenteeritud) tarkvara kasutamisel peab arvestama, et üldjuhul on tegemist tunduvalt nõrgema turvalisusega ja võimalusel seda vältida. Täpsemad soovitused ja nõuded nii arvutiklassidele kui ka esitlustehnikale leiab siit.

HITSA pakub huvilistele salvestustarkvara ECHO360 teenust ja võimaldab Nutiklassis tutvuda tänapäevaste tehnoloogiliste seadmete abil innovaatiliste õppemeetoditega. Nutiklassis on kasutusel kaks interaktiivset dataprojektorit, millega saab kuvada siledale pinnale puutetundlikku pilti, samuti proovida õppeprotsessi rikastamiseks mitmeid tahvelarvuteid ja nutitelefone ning programmeerimiseks LEGO robotikakomplekte. Lisaks leiab õpetajatele mõeldud veebipõhisest ProgeTiigri kogumikust vahendeid õppetöös

rakendamiseks. Materjale on järgmistest valdkondadest: programmeerimine, robotika, 3D-disain, nutiäpid ja multimeedia. Kogumik täieneb igal aastal.

3.1.1. Printimine

Arvutitöökoht on tavaliselt seotud **printimisteenusega**, mis võimaldab kasutajal vastavalt määratud kasutajaõigustele printida või paljundada vajalikke materjale. Printimisteenus peab olema kasutatav kogu asutuse piires (sisevõrk, *Virtual Private Network*, (VPN)) eri seadmetest kõikidesse asutuse võrguprinteritesse. Printimislahenduse jaoks vajalik tarkvara võib olla nii kohalik kui ka teenusena välise teenusepakkuja juures, aga keskselt hallatav, monitooritav (võib olla lahendatud teenusepakkuja poolt) ning kaetud hoolduslepinguga. Printimisteenuse katkestuseks ei loeta tavaliselt olukorda, kus printeris on lõppenud paber (mille tagamine on tavaliselt haridusasutuse halduspersonali ülesanne) või kui on takistatud üksiku printeri töö, kuid on võimalus printida teise mõistlikul kaugusel asuva printeri kaudu.

Soovitav on kasutada põhiliselt keskselt hallatavaid multifunktsionaalseid printereid ja vähendada eraldiseisvate väikeste A4-printerite osakaalu. Teenust ja selleks vajalikke seadmeid on riigikoolidel kohustus hankida Registrate ja Infosüsteemide Keskuse keskse raamhanke kaudu. Võimalusel soovitame printimist minimeerida või vältida ja selle asemel võtta kasutusele pilvepõhine vabatarkvara, mis võimaldab võrgupõhist koostööd ja aitab vältida tootjalukustusest tulenevaid probleeme.

3.1.2. Pahavaratõrje

Arvutitöökohtal peab olema tagatud **pahavaratõrje**. Pahavaraks, ka **kurivaraks** nimetatakse sellist tarkvara, mida kasutatakse ilma kasutaja teadmata tema arvutisse tungimiseks ja/või selle kahjustamiseks. Pahavara on mitut liiki: viirused, troojalased, ussid, nuhkijad, helistajad, reklaamijad jpm. Pahavaratõrje peab olema rakendatud kõigile väljastatud lõppseadmetele, k.a kõikidele füüsilistele ja virtuaalsetele serveritele. Kasutaja ei tohi saada pahavaratõrjet välja lülitada, see peab olema regulaarselt (vähemalt kord kvartalis või vajadusepõhiselt seoses juhtunud turvaintsidentidega) keskselt süsteemiadministraatori poolt kontrollitav ja hallatav, ajakohane ja uuendatav. Viirusetõrje peab ennast uuendama vähemalt kaks korda päevas, vastasel juhul ei pruugi kõiki ründeid avastada ja tõrjuda. Keskne haldamine võimaldab rakendada infoturbe meetmeid ja vajadusel operatiivselt tõkestada pahalaste rünnakuid (näiteks lülitada seadmeid võrgust välja jmt).

3.2. Kasutajate isikutuvastus ja -õiguste haldamine

Intellektuaalse omandi ja andmete turvalisuse tagamiseks peab olema selge, milline kasutaja pääseb ligi millistele ressurssidele. Tasub mees pidada, et kasutajale võib anda vaid tema tööülesannete täitmiseks vajalikud kasutajaõigused. Tähtajalise töö- või praktikasuhte puhul on mõistlik määrata kasutajate ligipääs tähtajaliselt ning võtta ligipääsud ära viimasel kooli- või tööpäeval. Kasutajaõiguste haldamine hõlmab kõigi kasutajat puudutavate IT-teenuste (sh rakenduste ja infovarade) juurdepääsude reguleerimist: kasutajale juurdepääsude, kasutajakontode või -rollide andmine, muutmine, sulgemine.

Isikutuvastuslahendused võimaldavad kasutajate autoriseerimist ja õiguste määramist koos ligipääsude võimaldamisega erinevatele IT-ressurssidele (tarkvara, seadmed, riistvara) nii sise- kui ka välisvõrgu (sh pilveteenuste) piires. Isikutuvastuslahendus peab sisaldama üldist infot kasutaja kohta, tema õiguste loetelu, ligipääsu erinevatele ressurssidele jne. Kahe üheaegse isikutuvastuslahenduse kasutamisel peavad need olema omavahel sünkroniseeritud (näiteks *Active Directory Federation System, ADFS*). Isikutuvastusteenus peab olema seotud ühtset logimist (*Single Sign-On, SSO*) ja infovahetust võimaldavate lahendustega (näiteks *ADFS, HarID, TAAT*, eesti.ee SSO jmt).

Isikutuvastuslahendus võib olla lahendatud nii lokaalselt kui ka majutatud teenusena, kas kohaliku teenuse pakkuja juurde või pilveteenusena (nt *Google Accounts, MS Azure AD*). Kasutajaid (näiteks õppurid), kellel pole vajadust omada ligipääsu asutuse sisevõrgu ressurssidele, tuleb eelistatult tuvastada välises (pilve)lahenduses.

HITSA pakub haridusasutustele identiteedilahendust HarID, mis on lihtsasti kasutatav isikuandmete ja kasutajakontode haldamise süsteem. HarID on mh keskne portaal andmete haldamiseks, kuhu sisestatud andmeid saab mugavalt saata riiklikesse andmebaasidesse, erinevatesse õpikeskkondadesse ja/või asutustele. HarID võimaldab ühtset sisselogimist, mis haridusvaldkonna riiklikele teenustele muutub kohustuslikuks. See sobib nii asutustele, kus kasutajakontode haldus puudub täielikult, kui ka juba olemasolevate lahendustega integreerimiseks.

Korrektne kasutajaõiguste haldamine aitab ellu viia infoturbepoliitikat ehk tagada andmete konfidentsiaalsus, terviklikkus ja käideldavus (vt lisaks peatükist Infoturve). Toodud põhimõtetele vastav isikutuvastuslahendus suurendab turvalisust (mitme konto asemel üks), seob IT-teenused tervikuks ja võimaldab kulude kokkuhoidu tänu väiksemale füüsilisele taristule ja ajaressursile, mis säästetakse kontode haldamiselt.

3.3. E-post, kalendri, postiloendite ja grupitöö lahendus

Lihtsustatult võimaldab e-postiteenus saata ja vastu võtta elektroonseid kirju ning sinna juurde kuuluv grupitöölahendus hallata haridusasutuse töötajate ja nõupidamisruumide ressursside kasutamist, kontrollida ülesannete täitmist jms. Täpsemalt peab teenus võimaldama e-posti saatmist ja vastuvõtmist, postiloendite loomist ja kasutamist; sünkroniseeritud kalendrit, mida saavad näha kõik sama lahendust kasutavad kasutajad või ka määratud välised kasutajad; ressursside broneerimist (seadmed (näiteks tahvelarvutid), ruumid, sõidukid vmt). Lahendus peab kasutama kasutajate autoriseerimiseks kesket isikutuvastust. Tavapärastelt luuakse igale kasutajale konto ja personaalne e-postiaadress kujul eesnimi.perenimi@haridusasutus.ee.

Mõistlik on luua teenusele veebipõhine ligipääs (näiteks *Outlook Web Access, SquirrelMail, Roundcube*, vmt) ja tagada kasutamine erinevates (mobiilsetes) rakendustes (näiteks *Outlook, Thunderbird, Google Mail ja Calendar, MS Exchange, Mail* jmt), samuti tulenevalt kasutaja töö iseloomust leppida kokku e-kirjade mahupiirangus (näiteks 5–20 MB) ja

postkasti kogumahus (näiteks 1 GB), konto sulgemise ning andmete säilitamise ja kustutamise tingimustes.

Pane tähele, et tulenevalt kasutajagruppide (õpetaja, administratiivtöötaja vs. õpilane) vajadustest võib siin kokku leppida erisusi teenuse sisule ja tingimustele. Näiteks kui õpilasele on loodud e-postiaadress haridusasutusega info vahetamiseks, siis ei pea talle võimaldama kooliressursside broneerimist (ruumid, sõidukid vmt), kontaktide töötlemist ega tööülesannete haldamist, mis pigem on vajalikud administratiivtöötajatele. Hea praktika näeb ette, et kasutaja e-postiaadress ja -konto suletakse viimasel kooli- või tööpäeval ning kuu hiljem kustutatakse lõplikult.

Põhimõtetele vastav lahendus annab kasutajale laialdased võimalused suhelda vajalike osapooltega ühises süsteemis, mis üldiselt aitab kaasa infohaldamise turvalisusele.

3.4. Failide hoidmine

Struktureeritud ja õigustega reguleeritud failide vahetamise ja hoidmise teenus annab kasutajale võimaluse salvestada oma töödokumente turvalises ja hallatud keskkonnas. Kokku on lepitud failipuu struktuur, kus igale kasutajale või -grupile on antud kindlad õigused failide vaatamiseks, muutmiseks ja/või koostamiseks ning rakendatud on versioonihaldus ja kasutajate autoriseerimiseks keskne isikutuvastuslahendus.

Kõiki digitaalsete töömaterjalide tuleb hoida nende säilimise ja andmete turvalisuse tagamiseks kataloogides, mis on sünkroniseeritud võrgukettale ja millest tehakse automaatseid varukoopiaid (vt varundamine). Töökohaarvuti töölaual (*desktop*’il) failide hoidmine ei ole soovitatav. Isiklikesse ja ühiskaustadesse mistahes tarkvara (mänge, programme, programmiuuendusi jne v.a süsteemide kriitilisi uuendusi) ning elektroonses vormis andmete (muusika, tekst, pildid, filmid jms) salvestamine ei ole üldiselt lubatud, v.a juhul, kui mainitud tegevus kuulub kasutaja tööülesannete hulka.

Asutuse sisemise andmekeskuse olemasolul lahendatakse failide hoidmine kohaliku failikettana (mis võib olla majutatud välises keskkonnas). Koolis peetavate serverite halduskulude vähendamiseks on eelistatud välised failide hoidmised. Seega võib täiesti iseseisva teenusena kaaluda failide pilvepõhist hoidmist (näiteks *OneDrive*, *Google Drive*, *SharePoint Online*, *OwnCloud*, *NextCloud*, *Dropbox* jne), **unustamata seejuures kehtivatest Isikuandmete kaitse seadusest ja Avaliku teabe seadusest tulenevaid andmete töötlemise nõudeid** (vt peatükki Infoturvet).

Siiski tuleb meeles pidada, et üldiselt ei ole avalikud pilveteenused turvalised ning andmed tuleb enne pilve panekut krüpteerida piisavalt kõrge (vähemalt 256-bit AES) krüptoga. Võimalusel soovitame käivitada oma isiklik pilv (näiteks *NextCloud*) ja kasutada seda.

Isikuandmete kaitse seadus defineerib isikuandmed, sh delikaatsed, mida haridusasutused töötlevad, näiteks andmed õpilaste tervises seisundi kohta. Isikuandmeid tuleb kaitsta tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest organisatsiooniliste,

füüsiliste ja infotehniliste turvameetmete rakendamise läbi. Sellised kohustused isikuandmete töötlejale (ehk haridusasutuse personalile) peavad olema defineeritud kooli sisemistes dokumentides (nagu sisekord, ametikirjeldus, tööleping).

Avaliku teabe seadus defineerib, millist infot tohib avaldada (nii kooliveebilehel kui ka failide näol erinevates pilveteenustes. Iga info avaldamisel tuleb analüüsida, milline info peab olema avalikult kättesaadav ja milline isikuandmete puutumatus huvides konfidentsiaalne. Piiratud ligipääsuga andmete vahetamiseks tuleb andmed krüpteerida (vt rohkem Infoturbe alajaotisest.)

3.5. Telefonside

Teenus annab kasutajale võimaluse kasutada helistamist ja sellega seotud teenuseid (kõnede suunamist, kõnede noppimist, laua- ja mobiiltelefoni numbrite ühendamist jmt) ning tihti kasutada erinevaid andmesideteenuseid. Lauatelefonide puhul soovitame kasutusele võtta välise ehk ilma kohaliku keskjaamata lahenduse, soovitatavalt interneti- ehk VoIP-põhine (*Voice over Internet Protocol*) ja kasutama SIP-protokolli (*Session Initiation Protocol*). Telefoniaparaadid võivad olla nii asutuse omandis kui ka väliselt teenusepakkujalt renditud, ent internetipõhise telefonside kasutamiseks peab asutuse välise võrguühenduse kiirus olema vähemalt 100 Mbit/s. Mõistlik on kasutajatele võimaldada laua- ja mobiiltelefoninumbrite ühildamist. Tööandja (haridusasutus või koolipidaja) võib kaaluda isiklike mobiilide kasutamise kompenseerimist vastavalt võimalustele, sõlmides lepingu välise teenusepakkujaga.

3.6. Kaugligipääs

Teenus võimaldab ligipääsu sertifitseeritud kanali ja terminaliserveri kaudu haridusasutuse sisevõrgus paiknevatele ressurssidele ja teenustele, nagu näiteks siseveeb/*intranet*, failiserver, e-post jne. Tavaliselt ei loeta kaugtööks elektronposti ja kalendrisüsteemi kasutamist läbi veebilehitseja (*browser*) väljaspool haridusasutust. Kaugligipääsu seadistamisel tuleb infoturbe meetmeid rakendada eriti hoolikalt, sest teenus on üldjuhul avatud kogu maailmale (internet) ning volitamata juurdepääsu eest tagavad kaitse vaid turvaliselt seadistatud tänapäevased uuendatud riist- ja tarkvaralahendused ning selle regulaarne hooldus.

3.7. Videokonverents

Videokonverentsi teenus võimaldab kokkulepitud geograafiliselt eraldatud ruumides korraldada samaaegseid ühendatud töökohtumisi. Videokonverentsi teenuse planeerimisel või sisse ostmisel tuleb arvestada järgmiste märksõnadega: koosvõimelised seadmed, virtuaalne koosolekuruum (*multipoint*), korralik helisüsteem (kõlarid, mikrofonid) ja esitluste näitamise ja jagamise võimalus. Lahendus peab toetama avatud standardeid.

Koosolekuruumides kasutamiseks mõeldud Full-HD lahutusvõimega (1920 x 1080) videokonverentsiseade peab toetama nii videoühenduse (H.263, H.264 ja H.239 (Polycom ühilduv) kui ka audioühenduse standardeid (G.711, G.722, G.722.1, G.728 ja kas G.722.1C või AAC-LD); võimaldama H.323 ja SIP kõnede ühenduskiirust vähemalt 4 Mbit/s; hõlmama vähemalt kahte video- ja kahte audiosisendit ning kahte mikrofoni; omama vähemalt kahte digitaalset videoväljundit (DVI, HDMI). Seadme haldamine peab olema võimalik nii veebiliidese kui ka kaugjuhtimispuldi kaudu; võrguliides peab olema nii IPv4 kui ka IPv6 võrguühenduse toetusega.

2016. a mais korraldati riigihange riigigümnaasiumite õppetehnika hankimiseks ja paigaldamiseks, mis muu hulgas kirjeldab ära detailsed nõuded videokonverentsiseadmele.

3.8. Infoturve

Kasvav sõltuvus IT-lahendustest sunnib järjest enam pöörama tähelepanu seotud infovarade (s.o andmete, tarkvarade, seadmete, personali, kasutajate ja füüsilise keskkonna) kaitsmisele (vt ka joonis 2). Selle ülesande täitmiseks **peab igal asutusel olema täidetud infoturbejuhi funktsioon**, mida võib eraldi inimese puudumisel täita mõni teine asutuse töötaja, samuti võib infoturbejuht olla mitme asutuse peale ühine või tellitud välise teenusena. Infoturbe tagamise **tegevused tuleks lisada asutuse üldisesse tegevuskavasse ning koolijuhi tasemel kontrollida selle täitmist**.

Infoturve ehk andmekaitse tähendab andmete kolme põhiomaduse – tervikluse, käideldavuse ja konfidentsiaalsuse tagamist, kus:

- **käideldavus** tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
- **terviklus** tähendab, et info pärineb usaldusväärsest allikast ning seda ei ole volitamata muudetud ega kustutatud;
- **konfidentsiaalsus** tähendab, et informatsioon on kättesaadav vaid volitatud isikutele.

Koolijuht koos infoturbe korralduse eest vastutava töötajaga peavad erilist tähelepanu pöörama: a) isikuandmete kaitsele, b) päevikute, hinnetelehtede ja dokumentide tervikluse tagamisele ning c) IT-lahendustest sõltuvate (sisseastumine, eksamite tegemine) kriitiliste tööprotsesside talitluspidevusele ja riskide maandamisele.

Infoturbe haldus on protsess, mis kindlustab organisatsiooni varade, info, andmete ja IT-teenuste konfidentsiaalsuse, terviklikkuse ja käideldavuse. Infoturbe tagamisel on võimalik eeskju võtta kehtivatest praktikatest. Tavaliselt hõlmab see: infovarade väljaselgitamist, riskianalüüsi, turvameetmete planeerimist ja rakendamist, toimepidevusplaani koostamist, avariiolekordade lahendamise harjutamist, koolitamist ja regulaarset hindamist.

Eesti riigiasutustes ja kohalikes omavalitsustes rakendatakse andmetele piisava tasemega turvalisuse tagamiseks infosüsteemide kolmeastmelist etalonit turbe süsteemi ISKE. Tegemist on valdkonnaspetsiifilise ja detailse tehnilise tekstiga, mis sobib lugemiseks IT-taustaga

inimesele. Riigi Infosüsteemi Amet on koostanud ka infoturbe soovitude juhendi, mis on konkreetne ja hea sissejuhatus IT-turvalisuse maailma. Juhend on mõeldud infoturbe valdkonna eest vastutajatele, juhtkonnale ja töötajatele, kes soovivad saada ülevaadet olulisematest infoturbemeetmetest ja olukorra hindamisest oma asutuses.

Küberrünnakud toimuvad pidevalt, näiteks Karspersky Labor pakub reaajas infot maailmas, sh Eestis toimuvate viirusrünnakute kohta. Nende statistikast nähtuvad peamiste küberohtudena erinevate nimedega pahavara (viirused, troojalased, nuhkvara jne) levik, rämpsposti (*spam*) saatmine ja e-postirünnakud ehk andmepüük (*phishing*), aegunud tarkvara haavatavused, häkkimine (*hackers*) ning sisemised ohud (*internal threats*). PricewaterhouseCoopersi uuring nimetab lisaks andmekao ning nõrkade paroolide ja irdmeedia⁶ (*removable media*) kasutamise.

Kõige levinum viis andmete kompromiteerimiseks on kaotatud või varastatud süle- ja tahvelarvutite, nutitelefonide või USB-pulkade kasutamine. Seadmete ja neis sisalduvate andmete füüsilise turvalisuse tagamiseks tuleb nii kontoris kui ka väljaspool seadme juurest kasvõi hetkeks lahkudes ekraan alati kaitsta parooliga ja lukustada, vältimaks volitamata juurdepääsu konfidentsiaalsele infole. Töö tegemiseks kasutatavaid seadmeid ei tohi jätta autosalongi istmele, vaid tuleb paigutada pagasiruumi. Nende põhimõtete järgimine kaitseb (mobiil)seadmeid ja andmeid lubamatu ligipääsu eest sinu eemaloleku ajal. Samuti ei tohiks töötegemiseks kasutada sõbra või avalikku arvutit, kuna ei saa kindel olla nende arvutite turvalisuses ja viirustõrjes.

Teiseks, kõik tundlikud andmed, mida säilitatakse lubatud kaasaskantavates seadmetes (näiteks sülearvutites, nutitelefonides), tuleks informatsiooni kaitsmiseks krüpteerida (*encryption*). E-posti saatmisel ja/või veebilehtede külastamisel on krüpteerimata info lihtsasti juurdepääsetav ja loetav, sest vaikumisi on kõik andmed kättesaadavad pealtkuulamiseks kõigile. Krüpteerimine teisendab informatsiooni juhuslikeks andmeteks, mis pole arusaadav ilma vastava võtmeta. See võti avab või lukustab andmeid sarnaselt füüsilise võtmele, mis sulgeb ja avab uksi. Krüpteeritud sõnumit on võimalik saata interneti teel, muretsemata, et keegi soovimatu saaks seda pealt kuulata või lugeda. Krüpteeritud andmete kaitsmiseks tohib ainult sinul olla juurdepääs vastavale võtmele. Eriti väärtuslikuks osutub krüpteerimine seadme kaotamise või varastamise korral. Krüpteerida on võimalik kõikvõimalikke mobiilseadmeid, näiteks nutitelefone, süle- ja tahvelarvuteid, USB-pulkasid, samuti külastades konfidentsiaalseid veebilehekülgi (nagu oma internetipanka või mõnda e-poodi), erinevaid suhtluskanaleid, näiteks e-posti, internetis tehtavaid kõnesid ja sõnumsidet.

Üldiselt tasub meeles pidada, et avatud standarditel töötavaid IT-lahendusi peetakse turvalisemaks, kui suletud ja patenteeritud süsteeme, kuna ei ole võimalik veenduda neis sisalduvaga.

⁶ Irdmeedia – arvutiga ühendatavad ja kaasaskantavad seadmed, nagu USB-pulgad, mälukaartid, aga ka digitaalne fotoaparaat, nutitefon, muusikamängija.

4. TARISTU TEENUSED

Taristu (ehk peamiselt riistvaraga seotud) teenused on vajalikud eespool nimetatud kliendispetiifiliste- ja IT-teenuste toimimiseks. Levinumateks näideteks majutamine (selleks vajalik piisav jahutus, elekter ja ruumid), varundamine jms. Oluline on mitte unustada, et iga soetusega kaasnevad iga-aastased hoolduskulud, mida eelarve planeerimisel tuleb arvestada. Ka taristu teenuste puhul tuleks kindlasti mõelda tootjalukustuste vältimisele ja vabavara kasutamisele.

4.1. Andmete ja serverite majutamine

Kõikide asutuse teenuste (postkastid, failihoidla, varundus, veebilehed, infosüsteemid jt) juures tuleb langetada otsused, kus ja kuidas neid majutada. Võimalusi on mitu:

- 1) paigutada teenused serverisse, mis asub füüsiliselt asutuse serveriruumis;
- 2) paigutada teenused virtuaalserverisse asutuse enda või mõne teenusepakkuja virtuaalserverite klastris;
- 3) võtta tasuta või tasuline teenus väliselt teenusepakkujalt;
- 4) kombinatsioon eelmistest.

Kindlasti tuleb enne otsuse tegemist arvestada järgnevaid kaalutlusi.

Füüsiliste serverite pidamine (tagades vastavuse kõikidele infoturbe nõudmistele) on kulukas, eeldades spetsiifilisi tehnilisi teadmisi ja võimekust tulla toime hädaolukordadega. Füüsiliste serverite arv koolis on kasulik viia miinimumini.

Vajalike füüsiliste serverite arvu saab teinekord vähendada, võttes kasutusele virtualiseerimise. Teisalt lisab see taristule keerukust, mistõttu on virtuaalserverite klastri ehitamine mõistlik ainult erandjuhtudel. Näiteks kui haridusasutuse põhitegevus on väga IT-mahukas – õpetatakse virtuaalserverite ehitamist ja haldust või kui õppetöö nõuab kümnekonna või enama virtuaalserveri kasutamist. Virtuaalserverite klastri ehitamisel tuleb valida sobiv tarkvara (HyperV, Proxmox, VMWare jt), arvestades seejuures nii litsentsitasude kui ka püsivate hoolduskuludega (sh kvalifitseeritud süsteemiadministraatori töö). Spetsiifilisi tehnilisi teadmisi ja oskusi nõudvate ülesannete täitmisega on alati seotud inimtööjõu konkurentsist ja volavusest tulenevad riskid (kompetentsi defitsiit ja kättesaadavus). Kuna perioodiliselt korduvad kulud võivad olla märkimisväärsed, peab otsus olema langetatud haridusasutuse juhtkonda ja omanikku kaasates.

Nii füüsilise serveri kui ka virtuaalserverite majutamisel tuleb arvestada turvanõuete täitmisega. Lähtudes ISKE metoodikast, tagab andmetele ja infosüsteemidele turvaosaklasside määramine, et asutuses on teadvustatud riskid ja võetud kasutusele elementaarsed meetmed nende maandamiseks. Asutuse sisemised teenused (failiserver, domeenikontroller jmt) on mõistlik siiski majutada asutuses, eriti juhul kui internetiühendus on madala kvaliteediga (vähese läbilaskevõime või sagedaste riketega). Kohaliku andmekeskuse olemasolul peab haridusasutuste serveriruum vastama vähemalt ISKE tasemele L. Vaata lähemalt RIA koostatud andmekeskuse turvanõuete [juhendist](#).

Ka teenuste sisseostmisel või majutusel välise teenusepakkuja serverites tuleb teadvustada kõik sellega seotud riskid. Kindlasti peab analüüsima eri teenusepakkujate lepingutingimusi, sest lisaks hinnaerinevustele võivad otsuse langetamisel määravaks osutada teenusepakkuja vastutus, klienditoe olemasolu, varundus, andmete taastamine jpm tegurid. Teenuste majutusel soovitame lepingusse lisada operatsioonisüsteemi hoolduse. Varunduse peab tagama juba teenuse käivitamise hetkest. Arvestada tuleb ka keskkondade, serverite ja rakenduste regulaarse uuendamise ja turvapaikamisega.

Isikuandmete, eriti delikaatsete isikuandmete, käitlemisel tuleb jälgida Andmekaitse Inspeksiooni juhendeid. Delikaatsete isikuandmete majutamisel välisriigis asuvates serverites või välisriigis registreeritud teenusepakkuja juures tuleb teadvustada, et võimalus kohustada teenusepakkujat järgima Eesti seadusi on piiratud, kontrollimine keerulisem ega saa kindel olla andmete töötlemise ja säilitamise turvalisuses.

Igal juhul tuleb teenuste majutamisel tehtud otsused dokumenteerida ja perioodiliselt üle vaadata, kuna muutuvad nii IT-teenuste hinnad ja teenusepakkujate portfellid kui ka asutusesisesed nõuded teenuste käideldavusele ja turvalisusele.

4.1.1. Varundamine

Õppetegevuse ja haridusasutuse kestlikkuse tagamiseks tuleb kõiki organisatsiooni infosüsteeme, andmeid ja riistvara (nii füüsilisi kui ka virtuaalseid servereid) regulaarselt (päevane/nädalane/kuine/aastane või muu kokkulepitud tsükkel) varundada. Varundamise reeglid ja põhimõtted tuleb dokumenteerida. IT-teenuse sisse ostmisel tuleb varundamise nõuded reguleerida teenusleppes.

Tavaliselt on varundamine automatiseeritud ja varukoopiaid hoiustatakse perioodiliselt mitmes asukohas (sh väljapool asutuse territooriumi). Varukoopiaid tuleb hoiustada viisil, mis välistab selle kiire riknemise (NAS seadmete puhul kasutada ketastel RAID6 andmeliiasust, lintide puhul hoida linte serveriruumist eraldi asuvas ruumis, pilveteenuse kasutamise korral valida selline teenus, mis tagab andmete säilimise eelpooltooduga võrreldaval tasemel). Varukoopiaid tuleb kontrollida mitte harvemini kui kord aastas, tehes selleks proovitaastamise.

Varundus peab olema ökonoomne, koormamata liialt töötavaid servereid, võrku ja varundusseadmeid/-teenust. Lahendus peab võimaldama nii süsteemset kui failipõhist, k.a kasutajapoolset, taastet, säästma võrguühendust ja võimalusel olema hallatav veebirakenduse kaudu. Soovitame kasutada versioonitud varundust, kus igal ajahetkel on säilitatud rohkem kui üks varukoopia.

4.2. Andmeside (kohtvõrgud ja wifi)

Andmeside toimimine ehk arvutivõrgu teenus on kõigi teiste IT-teenuste kasutamise vältimatu osa. Kohtvõrku ühenduvad nii kasutaja mobiilsed või statsionaarsed töökohad kui ka õppetöös vajalik esitlustehnika. Internetiühendus peab olema vähemalt 100 Mbit/s.

Klassikalise kaabliga andmeside teenuse puhul tuleb pöörata tähelepanu võrguseadmetele (kommutaator ehk *switch*) ja nende liidestele, tulemüüri seadmetele ja nende haldamisele, samuti kesksele haldusplatvormile ja kohtvõrgu kaabelduse paigaldusnõuetele. Üldised, tehnilised ja turvalisuse nõuded kohtvõrkudele, -seadmetele ja kaablitöödele on leitavad siit.

Traadita võrk (ehk wifi) on viimase viie aastaga kujunenud üheks peamiseks kasutatavaks teenuseks. See on õppetöös vajalik nii digitaalõppe populariseerimiseks kui ka informatsiooni kättesaamiseks, võimaldades haridusasutuse töötajatel, õppuritel ja külalistel pääseda interneti. Traadita andmeedastuskiirused on tehnoloogia arenguga jõudnud ajajärku, kus wifi tugijaamad suudavad edastada kiiruseid üle 1 Gbit/s (IEEE 802.11ac). See seab suurema rõhu kogu andmesidevõrgu baastaristule, mis peab olema suuteline teenindama kasvavat andmeside mahtu.

Wifi puhul tuleb arvestada nõudeid traadita võrgule ja seadmete paigaldusele, samuti traadita tugijaamadele (*Access Points*) nende arvu, mudeli ja asukohtade planeerimiseks. Kavandades uut wifi-võrku, peab peale levikattuvuse arvestama järjest kasvava nutiseadmete ja kasutajate arvu ning teenustega, mida võrgus plaanitakse kasutada. Koolide puhul on tegemist suure kasutajatetihedusega keskkonnaga, mis tähendab, et kasutajate arv on klassiruumides või üldkasutatavates ruumides (koridorid, aulad) keskmise kontori wifi-lahendusega võrreldes suurem. Seda peab arvestama ka tugijaamade mudelite valimisel, kuna seadmed peavad olema võimelised sellise kasutajate arvuga töötama.

Väljastpoolt asutuse sisevõrku peab ligipääs olema võimalik ainult turvalise VPN-ühenduse kaudu (*Virtual Private Network*). VPN-ühendus on krüpteeritud ja iga kasutaja on autenditud ning autoriseeritud.

Andmesideteenuse puhul on üks võimalus kasutada **eduroam** (ehk *Education Roaming*) lahendust, mis tagab, et kasutajad on autenditud ja autoriseeritud, samuti võimaldab panna kasutajaid eraldi võrkudesse – õpilased oma ja töötajad oma võrku, sh ligipääsuga kooli sisevõrku ning külalised oma võrku. See loob võimaluse, et õpetaja saab oma tahvli ja sülearvutiga olla kohe kooli sisevõrgus. *Eduroam* on projekt, mis võimaldab akadeemiliste võrkude kasutajatele vaba juurdepääsu internetile kõigis projektiga ühinenud asutustes.

4.2.1. Võrguseadmete haldamine

Halduskoormuse vähendamiseks on soovitatav kohtvõrgu haldamine teenusena sisse osta. Siin kirjeldatud lahendus võimaldab rakendada keskselt haldusmudelit, mis loob eeldused koolidesse paigaldatavaid seadmeid hallata ühest kesksest punktist (väline andmekeskus). Selline mudel lihtsustab seadmete ning teenuste monitoorimist (seiret), teenuse kvaliteedi jälgimist ning loob võimaluse ühtlustada turvapoliitikate rakendamist. Haldusmudeli keskne idee on standardiseerida võrgulahendus ning tagada koolide digitaristu kõrgem teenusekvaliteet. Lahenduse haldust on võimalik teostada rollipõhiselt, mis võimaldab luua erinevate õigustega kasutajate ligipääse halduskeskkonnale kooli- või piirkonnapõhiselt.

Kõik asutuse võrguseadmed (tulemüür(id), võrgukommutaatorid, wifi ligipääsupunktid ja wifi kontrollerseade või rakendus) peavad olema keskselt hallatavad vastavalt HITSA võrgustandardi määratud tingimustele, mis on leitavad siit. Asutustel tuleb tagada

võrguseadmetele toimiv monitooring ning kehtivate hoolduslepingute (seadmete garantii, haldus jne) olemasolu.

