TÖÖ PROGRAMM	**Kuupäev: 05.07.2024**	**Koostaja: Kristi Graf**	**Viide: B4**

Töö nimetus:	**Ülevaade KliM valitsemisalas väliste infovarade kasutamisest ja ligipääsuõiguste haldusest**
Eesmärk:	Toetada infoturvet, luua selgust ligipääsude andmise töökorralduses, toetada keskse identiteedi- ja pääsuhalduse (*Identity and Access Management*, IAM) rakenduse kasutuselevõttu.
Ulatus:	Väliste infovaradena käsitletakse IT-süsteeme, rakendusi, andmekogusid ja veebilehti nendele ligipääsuks jt IT-teenuseid, mida ei osuta KeMIT. Töö ulatusse ei kuulu kasutaja rollidega seotud küsimused (nt rakenduse kasutaja rolli, volituse vastavus tööülesannetele või rollikonflikt), füüsilised ligipääsud, logihaldus.

Teema taust

Töökohahalduse üks osa on juurdepääsuhaldus. Andmekogude ja rakenduste juurdepääsul lähtutakse minimaalõiguste põhimõttest[1] ehk pääs avatakse tööalase vajaduse korral, vähimas vajalikus ulatuses ja perioodiks. Infoturbe kõik põhikomponendid – konfidentsiaalsus, terviklus, käideldavus – seonduvad juurdepääsuhaldusega. Terviklik ülevaade tööks vajalikest pääsudest ja õigustest toetab infoturbe eesmärkide täitmist, võimaldab hõlpsalt hallata pääsude andmist ja eemaldamist ning kontrollida liigseid volitusi, avastada anomaaliaid, andmete lekkeid, identiteedivargust vm kuritarvitusi. Lisaks infoturberiskide maandamisele vähendab selge, läbipaistev õiguste haldus administreerimiskulusid, sest puudub vajadus igakordselt välja selgitada, kes ja mis protseduuri järgi avab vajaliku pääsu ning tagab tööks vajalikud andmed.

Seoses KliM loomisega ja E-ITS rakendamisega on vajalik uuendada valitsemisala üleselt pääsuhalduse alusinfo, uuendada töökorrad ja tagada protsessi tehniline tugi. E-ITS põhimõtetele vastava juurdepääsude halduse loomisega on alustatud[2], käesolev töö väliste infovarade osas annab sellele panuse töökohale vajalike rakenduste dokumenteerimisega.

Antud töö toimingud ja ajakava

Ettevalmistamise (eelselgituse) etapis, mais-juunis tutvuti pääsuhalduse korraldusega (sh intervjuud TRAM, EGT, RL, KeMIT-i esindajate ja KliM infoturbejuhiga), suheldi SMIT IAM projektijuhiga IAM kasutuselevõtmiseks vajalike andmete selgitamiseks, koostati ja eeltäideti infovarade tabel levinumate infovarade andmetega ja koostati tabeli täiendamise juhis.

Järgnevalt planeeritud tegevused juulis-augustis:

1. KliM valitsemisala asutuste tööks kasutatavatest valitsemisala-väliste infovaradest ja nendele ligipääsu andmetest ülevaate koostamine
   - Audiitor on koostanud eeltäidetud infovarade tabeli *Sharepoint*'is ja juhised tabeli täiendamiseks ning saadab need sisendinfoks asutuste kontaktisikutele, KliM-is osakondade juhtidele, referendile ja juhtkonna assistentidele.
   - Eelnimetatud tabel on oluliseks sisendiks antud tööle ja **täidetud tabelit ootame hiljemalt 26. juuliks**. Tabeli täiendamist oma andmetega koordineerivad KliM osakondade juhid ja asutustes kontaktisikud, kes jagavad asutuses infot tabeli täitmise vajadusest ja juhistest, koguvad andmed ja tagavad nende tabelisse sisestamise. Tabel täiendatakse iga asutuse ja KliM osakonna kohta eraldi[3].
   - Küsimus tööks kasutatavate infovarade kohta jõuab iga teenistuja või tema asendajani ja vastav info sisestatakse kaardistamise tabelisse – seda tagab asutuse koordinaator või KliM osakonna juhataja/ tema asendaja. KliM sisemises infokirjas jagatakse infovarade kaardistamisega seotud infot.
   - Andmete kogumise koordineerimine ja vajadusel jooksev juhendamine.

[1] *The least privilege principle*
[2] KliM infoturbejuhi eestvedamisel on taotletud rahastamist „Kasutajaõiguste ja identiteedi haldamise lahenduse kasutuselevõtu" projekti elluviimiseks. Taotlusvormil on projekti eesmärk „võtta kasutusele SMIT-i poolt arendatud IAM lahendus (SMIT saanud rahastuse RES taotluse kaudu 2022) ning seadistada see meie haldusala vajadustest lähtuvalt tööle.".
[3] Osakondade andmete eraldi kogumine on vajalik E-ITS rakendamiseks. E-ITS rakendatakse eelnevalt kaardistatud teenustele.

- Ülevaate põhjal sarnase pääsuhaldusega infovarade kirjeldamine, rühmitamine, võimalike riskikohtade tuvastamine ja parendusettepanekute tegemine.
- Ülevaate põhjal pääsuõigustega seotud tegevuste kirjeldamine, rühmitamine (etappide kirjeldamine) ja selle põhjal lihtsustamise ja standardiseerimise ettepanekute tegemine.

2. Pääsuhalduse protsesside toimivuse hindamine
   - Ülevaate põhjal koostatakse valim, millega testitakse igas asutuses ligipääsude õigeaegset sulgemist.
   - Testimise tulemuste võrdlemine kehtivate kordade ja sõlmitud lepingute nõuete nõuetega ning vastavalt sellele ettepanekute tegemine identiteedi- ja juurdepääsuhalduse kontrollide läbiviimiseks, kokkulepete muutmiseks.
   - Juurdepääsude halduse töökorralduse ja protseduuride analüüsimine.
3. Võimalike riski- ja kitsaskohtade tuvastamine ja analüüsimine ning parendusettepanekute tegemine.

Audiitorile vajalikud ligipääsud vastavalt valimile:

- infovara kasutuse aluseks olev lepingud vms alus dokument või võimaldada ligipääs asutuste dokumendihaldussüsteemi;
- teenistujate nimekiri, sh teenistussuhte algus- ja lõpukuupäevad asutuste personalitöötajatelt;
- infovara kasutajakontode nimekiri (pääsuloend) välise infovara omanikult (eelistatud variant) või valitsemisala asutuse teenistujalt, kellel on ligipääsude haldamise õigused, ligipääs KeMIT-i teenuste nimekirjale ja teenindusportaali ligipääsude haldamisega seotud piletitele.

Toimingud viiakse läbi mais kuni augustis, aruande eelnõu valmimine on planeeritud III kvartalis. Aruande eelnõu esitatakse asutuste kontaktisikutele faktivigade kontrolliks ja kommenteerimiseks ning toimingu tulemusel tehtud ja kokkulepitud parendustegevuste eest vastutavate isikute ja täitmise tähtaja määramiseks.

Töö läbiviija: Kristi Graf, *siseaudiitor*

/allkirjastatud digitaalselt/

Siseauditeerimise eest vastutav isik (AVI): Maarja Kilter, *siseauditi osakonna juhataja*

/*allkirjastatud digitaalselt*/

Lisa

Ligipääsudega seotud varasemad kontrollid

Aastal 2021. a viis KeM SAO läbi Infosüsteemide õiguste halduse korralduse kontrollitoimingu. Ilmnes KeM valitsemisala asutustes ca 200 infosüsteemi kasutamine, ca 5% sulgemata kontosid. Mitmed parendustegevused on KeMIT rakendanud, näiteks loodi automaatsed ühendused personaliandmebaasi ja IT-teenuse ligipääsu vahel, suurendatakse AD-ga liidestatud infovarade hulka, isikustamata AD kontode arv on minimaalne ja kasutaja tuvastatav.

Senine ligipääsude haldamine

Antud töö ettevalmistamisel ilmnes asutuste intervjuude põhjal, et kõikides asutustes avatakse teenistujale teenistuskoha struktuurist tulenev ligipääsude komplekt ja täiendavad ligipääsud taotletakse jooksvalt vahetu juhiga kooskõlastatult ja väliste süsteemide puhul enamasti e-kirjaga või KeMIT-lt Jira piletitga. Eristub KeA, kus on kasutusel teenistuskohtade lõikes infovarade ligipääsude tabel.

Käesoleva programmi koostamiseks eelselgituse käigus asutustega tehtud intervjuude kokkuvõtteks võib öelda, et IT-süsteemidele ligipääsude haldamine toimib suuresti usaldusel ja konkreetse peaksasutaja (õiguste halduri) kohusetundel, asutuste-üleselt ei ole pilti sellest, kellel ja kuhu on ligipääsud, samuti regulaarseid pistelisi kontrolle volitamata pääsude tuvastamiseks ei tehta. Logisid rutiinselt ei analüüsita, nendega tutvutakse, kui on esitatud (väline) päring andmetega tutvumise põhjuste kohta.

KeMIT-is ja TRAM-is toimib pöördumiste haldus Jira's, protsess ei ole kirjalikult kokku lepitud. Digitaalne identiteet ehk ülevaade töötaja kasutatavatest infovaradest on Jira süsteemist aruandena väljavõetav nende ITsüsteemide osas, milles toimub *Active Directory* (edaspidi AD) autentimine, kasutaja või infovara kaupa on leitav KeMIT poolt käsitsi lisatavate ligipääsude info (s.o. valitsemisala töötajate ligipääsusid finants- ja personalihaldustarkvarale SAP ja KeA-le vastavalt kaardistatud tabelile). Jira pileti süsteemis salvestatakse ligipääsu taotlus ja kooskõlastamine. Süsteemides, mis ei ole keskse ID võrgustikuga seotud, loovad/ taotlevad kasutajad endale ise kontod, kasutaja logib sisse tunnustega, mis ei ole seotud võrgu ID-ga.

Ligipääsudega seotud peamiste õigusaktide, standardite jt peamiste dokumentide nõueded

Küberturvalisuse seaduse alusel (KüTS) on sätestatud (digitaalse) teenuse ostutaja süsteemi tutvameetmed[4], täpsemalt Eesti infoturbestandard (E-ITS). E-ITS etalonturbe kataloogi (infoturbeprotsessi loomise ja käigushoidmise parimate tavade) moodul ORP.4: Identiteedi ja õiguste haldus sisaldab kokku 21 põhi- või standardmeedet (lisaks 3 kõrgmeedet). E-ITS järgi on kokkuvõtlikult üldisteks nõueteks kehtestada ligipääsude poliitika, organisatsiooni kasutajakontode ja paroolide halduse kord, õiguste haldamine rollipõhiste kasutajarühmade kaudu ja õiguste profiili pideva ajakohasuse tagamine. Profiili ajakohasuse tagamine tähendab õiguste vastavust tööülesannetele, minimalsele teadmisvajadusele, konto kasutuse kontrollimist ja kustutamist (deaktiveerimist, arhiveerimist) vastavalt muudatustele SAP personaliandmebaasis. Ligipääsude haldus IT-süsteemidesse ja rakendustesse sobitatakse äriprotsessidega ning tuvastus- ja autentimismehhanismid peavad vastama äriprotsessi kaitsetarbele (andmete, teenuse jms nõue). **Valitsemisala asutustes kavandatakse E-ITS põhi- ja standardmeetmete rakendamist**.

KüTS alusel on kehtestatud määrus Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel, mida kohaldatakse, kui KüTS § 3 lõikes 4 nimetatud *teabepidaja* kasutab AvTS § 3 lõikes 1 sätestatud avaliku teabe töötlemiseks: 1) andmetöötlusressursside kogumit, mis on paindlikult jagatav

[4] Teiste seas on § 7 lõikes 3 sätestatud Teenuse osutaja süsteemi turvameetmed. Kui teenuse osutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, **vastutab teenuse osutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise**.
Vastavalt seletuskirjale, lk 16: *„Lõige 3 sätestab teenuse osutajale kohustuse tagada süsteemi turvameetmete rakendamine ka juhul, kui süsteemi kasutamine volitatakse edasi teisele isikule. Sätte eesmärk on tagada, et **kõik missioonikriitiliste süsteemide kasutamisega seotud osapooled hoolitseksid süsteemi turvalisuse tagamise eest vajalikul, ettenähtud tasemel**. Sätte eesmärgiks on pöörata tähelepanu sellele, et teenuse osutaja peab sõlmima teenuse osutamiseks kasutatavate väliste osapooltega piisavad lepingud, mis hõlmaksid ka eelnõus sätestatud nõuete täitmist. Nõuete täitmise kohustus on teenuse osutajal ning järelevalve subjektiks on samuti vaid seaduse kohaldamisalas olev teenuse osutaja.“.*

ja laiendatav võrgu- ja infosüsteemi ennast muutmata ning millele pakub juurdepääsu /…/ valitsusasutus või valitsusasutuse hallatav riigiasutus (*avaliku sektori osutatav pilvteenus*); 2) pilvandmetöötlusteenust. Määruse kohaselt järgib teabepidaja pilvteenuse kasutamise kestel avaliku teabe käideldavuse, tervikluse ja konfidentsiaalsuse nõuete täitmist.

Vabariigi Valitsuse 25.05.2017 määrusega nr 88 Teenuste korraldamise ja teabehalduse alused reguleeritakse valitsemisala teenuste osutamist. Vastavalt § 4 lg 1 punktile 4 määrab asutus teenistuskoha(d), millel töötavad isikud tagavad asutuse teabehalduse iga alategevuse korraldamise ja kvaliteedi, teabehalduse üks alategevus on teabele juurdepääsu ja teabe kaitse korraldamine (§ 3 lg 1). § 7 lõike 10 kohaselt kui asutus haldab infosüsteemi, milles osutab või kasutab teenust teine asutus, vastutab ta tehnilise lahenduse ning selle toimimise ja arendamise eest. Infosüsteemi haldaja ja infosüsteemi kasutavate asutuste vahel lepitakse kokku: 1) infosüsteemi võimalused, nende **kasutamine** ja muutmine; 2) vastutuse jaotus protsessi ja teenuse kvaliteedi eest. *Kasutamine seejuures võib sisaldada ka juurdepääsuõigustega seonduvat, seejuures tulenevalt viidatud määrusest kasutajate haldamine võib olla nii infosüsteemi haldaja kui selle kasutaja tegevus, olenevalt konkreetsest kokkuleppest.* Vastavalt § 12 lõikele 3 määrab asutus põhiülesande täitmisel tekkivast teabest ülevaate saamiseks kindlaks:

1) millist teavet on põhiülesande täitmisega seotud teenuste osutamiseks vaja, lähtudes õigusaktiga sätestatud tingimustest;
2) millist lisateavet põhiülesande täitmisel ja teenuste osutamisel luuakse või saadakse;
3) millised on **teabe allikad**;
4) millistes vormingutes ja hoiukohtades teavet hoitakse;
5) millised on teabe säilitustähtajad ja **juurdepääsutingimused**;
6) kes on teabe kasutajad.

Vastavalt §-le 13:

(2) Asutus tagab, et riigi infosüsteemi haldussüsteemis (edaspidi RIHA) on ajakohased ja tõesed andmed selle kohta, **milliseid infosüsteeme ta teabe vastutava töötlejana haldab või kasutab**, ning et kirjeldus vastab kehtestatud nõuetele.

(4) Kui asutus haldab infosüsteemi, milles töötlevad teavet teised asutused, vastutab haldaja teabe säilimise, kasutatavuse ja kaitse, teabe avalikku arhiivi üleandmise või hävitamise ning **teabele juurdepääsu võimaldamise** eest.

(5) Teabele juurdepääsu võimaldamisel ning isikuandmete ja muu teabe kaitse korraldamisel lähtub asutus avaliku teabe seadusest ja andmekaitset reguleerivatest õigusaktidest ning arvestab koordineerija juhiseid.

(7) Kui asutus majutab teavet eraõigusliku isiku juures või volitab haldusülesande täitmiseks eraõiguslikule isikule, tuleb lepingus ette näha tingimused majutamise või haldusülesande täitmise käigus tekkiva avaliku teabe: 1) säilimise, kasutatavuse ja kaitse ning sellele juurdepääsu korraldamise kohta; 2) asutusele üleandmise korralduse kohta lepingu lõppemisel või eraõigusliku isiku tegevuse lõpetamisel.

Isikuandmete kaitse üldmäärus (GDPR) ja Isikuandmete kaitse seadus (IKS) täpsustab isikuandmete töötlemise turvameetmed ja andmekaitsespetsialisti rolli.

Valitsemisala-üleselt kehtivad varasemalt koostatud infoturbe kokkulepped ja korrad, mis KliM asutustes nagu TRAM, RL ja EGT ei pruugi kasutava praktikaga ühtida. KliM-s rakendatavad korrad eeldavad üldiste IT-korralduse kokkulepete (nt KeMIT roll lisandunud asutustes) järel rakendamist vastavalt E-ITS põhimõtetele. Seni kehtiva infoturbe poliitika (kantsleri 21.12.2018 kk nr 1-2/18/939) järgi koordineerib KeMIT valitsemisalas infoturbe haldust ja asutused tagavad personaliga seotud turvameetmete rakendamise (p 1.4), samuti deklareeritakse, et *Asutuste tõhusas igapäevases toimimises on infovaradel tähtis roll. Infovarasid tuleb kasutada ainult määratud otstarbel. Poliitika järgi* ***antakse juurdepääs infovaradele ainult tõendatud teadmisvajaduse alusel ja keelatakse juurdepääs neile, kellel selline vajadus puudub****. Asutuste juhtkonnas tegelevad infoturbega ning kohustavad infoturbenõudeid järgima kõiki teenistujaid.* (p 2). Valitsemisala infosüsteemide varad ehk infovarad on infotehnoloogilised vahendid ja nende abil töödeldavad anded ehk teave (p 3.1, p 3.2). Poliitika järgi infovaradele ligipääsu korraldab, vastutab ja kontrollib vara kasutajate tegevust

infovara omanik, andmekogu vastutava töötleja esindaja – audiitori hinnangul paralleelselt tõlgendades ka välise infovara puhul infosüsteemi peakasutaja vms on poliitika mõistes infovara omanik, kes peab tagama kasutuse vastavalt välise poolega sõlmitud lepingule. Poliitika järgi täidavad asutuste infoturbe eest vastutavad isikud oma asutuses vähemalt mh järgmisi kohustusi lähtuvalt infoturbenõuetest: *teavitavad teenistujaid valdkonna olulisusest ning tagavad, et kõik* ***töötajad oleksid oma infoturbe- ja isikuandmete kaitse alasest vastutusest teadlikud****, korraldades koostöös infoturbejuhiga koolitusi (p 5.8.3);/.../ korraldavad töö selliselt, et uue teenistuja andmed on edastatud personali eest vastutavale isikule ning kantud personalihaldustarkvarasse enne, kui talle tellitakse infovara kasutusõigused (p 5.8.5); korraldavad töö selliselt, et infovara kasutaja töökohustuste muutumisest või töösuhte lõppemisest teavitatakse kohe infovara kasutusõiguste andjat, tagamaks kasutajaõiguste õigeaegse muutmise või äravõtmise (p 5.8.6)*.

Riigilaevastiku värbamise ja valiku korra (23.02.2024 kk nr 1-1/24/5) kohaselt personaliüksuse koostatav **värbamistaotlus sisaldab ka tööks vajalike programmide, süsteemide infot**.