Vabariigi Valimiskomisjon

E-hääletamise süsteemi infoturbe poliitika

Versioon 2.1

Dokument: EHA-02-03-2.1

Kuupäev: 01.02.2015.a.

Redaktsioonide ajalugu

Kuupäev	Versioon	Kirjeldus ja muudatused	Autor
01.08.2005	1.0	Koostatud ja vastu võetud dokument.	Jaak Tepandi
21.04.2009	1.1	Kustutatud ebaolulist, sh. keeld sülearvutite kasutamisele.	
04.06.2012	2.0.0projekt	Põhjalik ümbertöötlus ja ISKE ver 6.00 vastavusse seadmine	Cybernetica AS (Ahto Buldas)
01.12.2012	2.0.1projekt	Redigeerimine lähtudes Priit Vinkeli ja Tarvi Martensi kommentaaridest	Cybernetica AS (Sven Heiberg)
19.09.2013	2.0	Kinnitatud versioon	Tarvi Martens
01.02.2015	2.1	Ajakohastatud	Tanel Kuusk

Sisukord

1. Sissejuhatus

1.1. E-hääletamise infoturbe olulisus

Elektroonilise hääletamise (e-hääletamise) turve on oluline nii Eesti riigi, demokraatia arendamise kui ka valijate privaatsuse seisukohast. Vabariigi Valimiskomisjon (VVK) ning Elektroonilise Hääletamise Komisjon (EHK) rakendavad kõiki asjakohaseid meetmeid e-hääletamise turbe tagamiseks ja nõuavad seda ka muudelt e-hääletamisega seotud isikutelt ja organisatsioonidelt.

1.2. Ülevaade

E-hääletamise turbe tagamisel on mitmeid eripärasid. E-hääletamise süsteem on aktiivne piiratud aja vältel ja on seotud erinevate osapooltega. Süsteemil ei ole kinnistatud personali, pidevalt eraldatud ruume, Internetiühendust jne. Samas peab e-hääletamise süsteem vastama Eestis kehtiva ISKE turvastandardi H-taseme nõuetele.

E-hääletamise süsteem on tundlik kasutatava tarkvara, riistvara ja teenuste usaldusväärsuse suhtes. E-hääletamise süsteem on hajussüsteem, koosnedes mitmest eri keskkondades töötavast komponendist, harva kasutatav, raskesti testitav ja aegkriitilise valmimistähtajaga.

Infoturbe poliitika eesmärk on esitada Vabariigi Valimiskomisjoni toetus infoturbele, määratleda infoturbe eesmärgid, organisatsioonilised ja infotehnoloogilised meetmed ning pakkuda tuge infoturbe juurutamisele ning selle tagamisele e-hääletamise käigus.

Infoturbe poliitika rakendusala on e-hääletamise organisatsioon ja e-hääletamisega seotud infotehnoloogilised süsteemid. Infoturbe poliitikas ei kirjeldata süsteemi ennast. Seda on tehtud dokumendis "E-hääletamise organisatsioon ja infrastruktuur".

1.3. Materjalid

Käesolevat infoturbe poliitikat tuleb lugeda koos teiste e-hääletamise kohta käivate dokumentidega (vt ülevaadet "E-hääletamise dokumentatsioon"). Kuna konfiguratsiooni- ja muudatuste haldust rakendatakse ka väljaspool infoturbe haldust, on vastavad protseduurid, aga samuti mõned muud infoturbesse puutuvad teemad, kirjeldatud dokumentides "E-hääletamise käsiraamat", "E-hääletamise organisatsioon ja infrastruktuur" ja mujal.

Lisaks mainitutele tuleb e-hääletamise infoturbe korraldamisel arvestada Eesti Vabariigi seaduste ja teistest õigusaktidega ning Riigikogu Kantselei kordadega (sealhulgas sisekorraeeskirja, asjaajamiskorra, asutusesisese teabe kasutamise korra ja Toompea lossis viibivate isikute ohuolukorras tegutsemise korraga).

Käesoleva dokumendi ülesehitus ja sisu põhineb standarditel "EVS-ISO/IEC 27001:2014. Infotehnoloogia. Infoturbe halduse süsteemid. Nõuded", "EVS-ISO/IEC 27002:2014. Infotehnoloogia. Infoturbemeetodite tavakoodeks", "EVS-ISO/IEC

12207:2009 Infotehnoloogia. Tarkvara elutsükli protsessid", ”EVS-ISO/IEC 27005:2014 Infotehnoloogia. Infoturvariski haldus” ning infosüsteemide kolmeastmelise etalonturbe süsteemil (ISKE-metoodikal).

1.4. Kasutatud mõisted ja lühendid

E-hääletamise süsteemi kriitilised riskid – e-hääletamise tulemuste ebakorrektsus, e-hääletamise tulemuste ebausaldusväärsus, hääletamise katkemine, hääle salajasuse rikkumine.

Kriitiline protseduur – protseduur või tegevus, mille valesti täitmine võib viia e-hääletamise kriitiliste riskide realiseerumiseni.

E-hääletamise süsteemi salajased andmed – süsteemi salajane võti, e-hääletajate poolt signeeritud ning krüpteeritud hääled, valimiste kodulehe ning HES TLS-serveri ja valijarakenduse koodi signeerimise võtmepaaride salajased võtmed, kontrollirakenduste signeerimise võtmepaaride salajased võtmed ja/või rakenduste poe pääsukoodid.

Kriitilised andmed – kõrge riskiastmega andmed (sealhulgas salajased andmed), mille allikat peab saama tõestada kolmandale osapoolele ja mille volitamatu muutmine või hävinemine võib viia e-hääletamise kriitiliste riskide realiseerumiseni.

Kriitilised seadmed – seadmed, mis töötlevad kriitilisi andmeid.

Turvaintsident – sündmus, mis võib kahjustada e-hääletamise informatsiooni või seadmete turvalisust (konfidentsiaalsust, terviklust või käideldavust), sealhulgas turvarike, oht, nõrkus või tõrge.

HES – Häälteedastamisserver.

HTS – Häältetalletamisserver.

HLR – Häältelugemisrakendus.

AR – Auditirakendus.

HSM – riistvaraline turvamoodul *(Hardware Security Module).*

VIS – Valimiste infosüsteem. Tegeleb nii e- kui paberhäälte lugemise koontulemuste kogumise, salvestamise ja töötlemisega. Ei loeta e-hääletamise infosüsteemi osaks.

Kesksüsteem – Vabariigi Valimiskomisjoni vastutuse all olev süsteemiosa. Tegeleb häälte vastuvõtmisega ja töötlemisega kuni e-hääletamise koondtulemuse väljastamiseni.

Valimiste koduleht – Vabariigi Valimiskomisjoni vastutuse all olev veebileht *www.valimised.ee*, esmane pöörduspunkt valijale.

Valijarakendus – E-hääletamise süsteemi komponent, mis töötab valija arvutis ja mille abil valija teostab oma valiku.

Kontrollirakendus – E-hääletamise süsteemi komponent, millega saab valija oma hääle kesksüsteemi talletumist kontrollida.

2. Turvaeesmärgid ja -põhimõtted

2.1. E-hääletamise turvaeesmärgid

E-hääletamise kõige olulisemad turvaeesmärgid on järgmised:

- *Korrektsus.* Hääletamise tulemus väljendab valijate tahet ja on kooskõlas kehtiva õigusega.
- *Usaldusväärsus.* Hääletamine on läbipaistev, auditeeritav, hääle arvestamine kontrollitav ja häälte loendamine korratav.
- *Salajasus.* Vaid hääletaja ise teab, kelle või mille poolt ta hääletas.
- *Kooskõla traditsioonilise hääletusviisiga.* E-hääletamine ei ole ainus valimistel kasutatav hääletusviis ja ühe ekstreemse turvameetmena nähakse ette ka e-hääletamise tühistamist koos traditsioonilisel viisil ümber hääletamisega. Tuleb tagada, et e-hääletamise õnnestumine või ebaõnnestumine ei ohustaks valimisi tervikuna. Tuleb tagada, et iga valimas käinu kohta läheks arvesse ainult üks hääl.

Olulised on ka paljud muud e-hääletamise protsessile esitatavad nõuded, laiemalt on e-hääletamise turvaeesmärgiks tagada nende täitmine. Vastavad nõuded on toodud dokumendi "E-hääletamise kontseptsiooni turve: analüüs ja meetmed" jaotises 2.2, dokumendi "E-hääletamise organisatsiooniline ja tehniline kontseptsioon" jaotises 2 ning dokumendi "E-hääletamise süsteemi üldkirjeldus" jaotises 2.

2.2. Põhimõtted

Infoturbe põhimõtted on järgmised:

- Kriitilistele seadmetele ja informatsioonile (vt jaotis 5) tuleb anda juurdepääs ainult tõendatud tööalase vajaduse alusel.
- Kriitiliste seadmete ja informatsiooni kaitse peab olema rakendatud sõltumatult nende asukohast.
- Kriitilisi protseduure sooritatakse vähemalt kahe EHK liikme koostöös ja töötajaid tuleb perioodiliselt roteerida. Sooritatud protseduuridest jääb auditeeritav jälg.
- Juurdepääs kesksüsteemi riistvarale ja tarkvara paigaldusmeediale antakse ainult tõendatud tööalase vajaduse alusel ja keelatakse kõigil teistel puhkudel.
- E-hääletamise kesksüsteemi riistvara ja tarkvara kasutatakse valimisperioodil ainult otseselt e-hääletamise läbiviimiseks vajalike ülesannete täitmiseks, kõik muud kasutusviisid on keelatud.

Tagamaks juurdepääs tõestatud vajaduse alusel, rakendatakse füüsilisi (pääsu reguleerimine, turvakleebiste kasutamine) ja loogilisi piiranguid (identimine ja autentimine).

ISKE H-taseme turvatundlikke andmeid ja seadmeid tuleb kaitsta nii füüsiliste kui loogiliste piirangutega. Muid andmeid tuleb kaitsta kas füüsiliselt või loogiliselt.

Valimiste koduleht paikneb majutusteenuse keskkonnas ning selle turbemeetmed on kirjeldatud teenusepakkuja turvadokumentatsioonis. Pakutav keskkond peab vastama peatükkide 8, 9, 13 ja 14 nõuetele. Keskkondade ligipääsuinfot hallatakse vastavalt käesoleva dokumendi punktidele 5.1 ja 5.3.1.

Kontrollirakendust levitatakse vastava mobiilse platvormi tootja (Apple, Google, Microsoft) ametliku poe vahendusel. Poodide kasutajatunnuseid ja salasõnu hallatakse vastavalt punktidele 5.1 ja 5.3.1. Poodide üldised turbemeetmed on kehtestatud vastava tootja poolt.

E-hääletuse perioodil paigutatakse kesksüsteemi serverid majutusteenuse pakkuja ruumidesse, kuna valimiste lühiajalisusest ja organisatsiooni väiksusest tulenevalt ei ole otstarbekas pidada eraldiseisvat füüsilist keskkonda. Kasutatav majutusteenus peab järgima käesoleva turvapoliitika põhimõtteid ja vastama toodud nõuetele. Majutusteenuse osa võib olla ka välisühendus ning selle turve (tulemüürid ja ründetuvastus).

3. Turbe organisatsioon ja infrastruktuur

3.1. Rollid, kohustused ja nõuete haldus

Elektroonilise Hääletamise Komisjoni esimees vastutab e-hääletamisega seotud rollide õigusaktidest tulenevatest nõuetest teavitamise eest.

Elektroonilise Hääletamise Komisjoni esimees vastutab infoturbe eest. Esimehe äraolekul asendab teda kohusetäitja, kes kinnitatakse EHK otsusega.

EHK esimehe roll on pidevalt täidetud ja tema kontaktandmed kõigile e-hääletamise süsteemi töötajaile kättesaadavad. Esimees on kogu tööpäeva jooksul kättesaadav ning valmis reageerima intsidentidele. E-hääletamise kriitiliste protseduuride täitmise perioodil (sh e-hääletamise ajal) on EHK esimees kättesaadav ööpäevaringselt.

EHK esimees määrab vajadusel teised infoturbega tegelevad rollid, sealhulgas

- täiendava turvaintsidentide haldaja,
- väliste lepinguliste osapooltega (näiteks majutusteenuse pakkujaga) seotud turvaintsidentide haldajad.

Ka nende rollide täitjad peavad e-hääletamise ajal olema kättesaadavad ning valmis reageerima kriitiliste intsidentide teadetele ööpäevaringselt.

Kõigi töötajate kohustused fikseeritakse kirjalikult: korraldusega, lepinguga või mõnel muul EHK poolt sätestatud moel.

EHK esimees määrab kontaktisiku e-hääletamise turvalisust käsitleva teabe edastamiseks avalikkusele, ja isikud avalikkuselt lähtuva turvateabe haldamiseks.

3.2. Turvapoliitikad

E-hääletamise organisatsiooni väiksuse tõttu on üleüldine turvapoliitika, e-hääletamise infoturbe poliitika ja e-hääletamise süsteemi turvapoliitika koondatud ühte dokumenti.

Muud infoturbega seotud dokumendid (talitluspidevuse plaan, konfiguratsioonihalduse kord, paroolide haldus, võtmete haldus jne) on vormistatud turvapoliitika alajaotistena.

4. Infoturbe ja riskianalüüsi strateegia

4.1. Infovarad

E-hääletamise süsteemi infovarad on esitatud Lisas A.

E-hääletamise süsteemis töödeldavad andmed on täpsemalt kirjeldatud dokumentides “E-hääletamise süsteemi üldkirjeldus” ja “E-hääletamise kontseptsiooni turve: analüüs ja meetmed“.

4.2. Riskianalüüs ja süsteemi turbeaste

Vajaliku turbetaseme määramisel lähtutakse ISKE etalonturbe metoodikast. Vajadusel viiakse läbi ka detailsemaid riskianalüüse. Dokument “E-hääletamise kontseptsiooni turve: analüüs ja meetmed“ esitab detailse tehnilise riskianalüüsi. Mõningad selle aruande esitamisest möödunud ajavahemikus aktuaalseks muutunud lisariskid on esitatud dokumendis "E-hääletamise süsteemi hinnang".

Lisaks käesolevale infoturbe poliitikale ning eespool mainitud dokumentidele on infoturbe haldusega seotud konkreetsemaid küsimusi kirjeldatud ka mitmetes teistes dokumentides (vt ülevaade "E-hääletamise dokumentatsioon").

Kuna e-hääletamise süsteemi väline IT keskkond on muutuv, tuleb riskianalüüsi perioodiliselt vähemal kord kahe valimise vahelisel ajal üle vaadata ning kaasajastada. Otstarbekas on teha seda e-hääletamise süsteemi hinnangute ja auditite käigus. Lisaks tuleb riskianalüüs üle vaadata siis, kui süsteemis või selle organisatsioonis tehakse suuremaid muudatusi.

4.3. Turbe vastavuse kontroll

E-hääletamise süsteemi organisatsiooni, infrastruktuuri ja tarkvara siseaudit viiakse läbi igakord enne e-hääletamise süsteemi kasutuselevõttu järjekordsel hääletamisel. E-hääletamise süsteemi organisatsiooni, infrastruktuuri ja tarkvara audit viiakse läbi perioodiliselt.

Kriitilised e-hääletamise protseduurid viiakse läbi koos välise audiitoriga.

5. Pääsu reguleerimine

5.1. Pääsuõigused

Alalise ja lepingulise personali pääsuõigused e-hääletamise kesksüsteemi seadmetele ja informatsioonile (sealhulgas luba seifi kasutamiseks ja seifi võtmete hoidmise kord) sätestatakse EHK otsusega.

Kolmandad osapooled e-hääletamise kesksüsteemi seadmetele või informatsioonile iseseisvalt ligi ei saa.

Iga kasutaja või kasutajarühma jaoks on olemas selgelt määratletud pääsu reguleerimise poliitika. See poliitika peab andma pääsuõigusi vastavalt tööalastele nõuetele. Üldpõhimõte on "nii palju õigusi kui vaja, nii vähe õigusi kui võimalik".

Lubamatu juurdepääsu vältimiseks arvutitesse, andmetele, teenustele ja rakendustele kasutatakse paroole. Iga volitatud kasutajat peab saama identida ja ta identiteeti kontrollida, kusjuures edukad ja edutud pääsukatsed logitakse.

Rakendustele lubamatu juurdepääsu vältimiseks kasutatakse rollipõhist pääsureguleerimist, mis võimaldab juurdepääsu vastavalt kasutajate tööülesannetele.

Pääsuõigused süsteemidele ja informatsioonile vaadatakse üle igakordselt enne süsteemi rakendamist valimistel. Kui pääsuõigused pole enam vajalikud, tuleb nad viivitamatult ära võtta.

Valimiste kodulehe, kontrollirakenduse levituskanalite ja VIS pääsuõiguste eest vastutavad vastavate keskkondade haldajad.

5.2. Füüsiline pääsu reguleerimine

E-hääletamise kesksüsteem paikneb erinevatel etappidel erinevates asukohtades:

- valimiste vahelisel perioodil – e-hääletamise kesksüsteemi haldaja ladustamiskeskkonnas,
- hääletuseelse perioodi alguses ning hääletusjärgse perioodi lõpus – e-hääletamise kesksüsteemi haldaja ladustamis- ja töökeskkonnas,
- hääletuseelse perioodi lõpus, hääletusperioodil ning hääletusjärgse perioodi alguses – häälteedastamis- ja häältetalletamisserverite majutaja keskkonnas, teatud süsteemi komponendid ja andmed võivad paikneda eri ajahetkedel väljaspool eelnevat kahte asukohta.

Ladustamiskeskkond on ruumid, kus hoitakse e-hääletamise süsteemi komponente ladustamise eesmärgil, väljalülitatud olekus. Salajaste andmete ja turvakriitiliste seadmete ladustamiseks tuleb kasutada seife või alternatiivseid meetodeid, mis tagavad tervikluse, konfidentsiaalsuse ja käideldavuse. FIPS 140-2 tase 3 ning Common Criteria EAL 4+ sertifikaadiga seadmeid võib hoida tulekindlas kapis, nende ründetuvastusindikaatoreid tuleb enne kasutamist kontrollida.

Töökeskkond on ruumid, kus e-hääletamise süsteemi komponendid on sisselülitatud olekus protseduuride läbiviimiseks.

Majutaja keskkonnas on e-hääletamise süsteemi komponendid 24/7 režiimis sisselülitatud ja toimimises.

Süsteemi ja andmete konfidentsiaalsus- ja terviklusnõuded kehtivad kõigis keskkondades. Käideldavusnõuded on olulisemad e-hääletamisel (majutaja keskkonnas).

E-hääletamise süsteem peab paiknema turvalistel aladel, mida kaitsevad määratletud turvaperimeetrid turbetõkete ja sissepääsu reguleerimise vahenditega. Turvaperimeeter on miski, mis moodustab tõkke, näiteks sein, kaartjuhitav sissepääs või mehitatud pääsla. Süsteem peab olema volitamatu juurdepääsu, kahjustuste ja häiringute eest füüsiliselt kaitstud.

5.2.1. Turvaline ala valimiste vahelisel perioodil

Valimiste vahelisel perioodil on elektroonilise hääletamise süsteem välja lülitatud olekus. Kaitstavate varade hulgas ei ole konkreetse valimisega seotud andmeid ja kesksüsteemi riistvara, tagada tuleb:

- E-hääletamise tarkvara lähtekoodi terviklus ja käideldavus.
- Riistvaralise turvamooduli terviklus ja käideldavus.

Turvaliseks alaks on e-hääletamise süsteemi haldaja ladustamiskeskkond. Kui riistavaralist turvamoodulit või e-hääletamise tarkvara lähtekoodi viiakse valimiste ajal turvaliselt alalt välja kolmandate osapoolte valdusesse, siis sõlmitakse kolmanda osapoolega leping, mis kohustab neid tagama varadele vähemalt samaväärse kaitstuse kui e-hääletamise süsteemi haldaja keskkonnas.

5.2.2. Turvaline ala valimiste ajal

Valimiste ajal ja valimistele vahetult eelneval ning järgneval perioodil on e-hääletamise süsteemi turvalised alad e-hääletamise süsteemi haldaja ladustamiskeskkond, töökeskkond ja majutaja keskkond.

5.2.3. Turvalise ala põhimõtted

E-hääletamise turvaline ala tohib paikneda hoones, mis on lukustatud ja kaitstud.

E-hääletamise ladustamiskeskkond ja majutaja keskkond peavad paiknema ruumides, mis on lukustatud ja kaitstud.

E-hääletamise töökeskkond peab olema lukustatud ja inimtühi, kui seal ei viibi korraga vähemalt kahte e-hääletamise süsteemiga töötama volitatud isikut.

E-hääletamise süsteemi turvalist ala sisaldava hoone perimeeter peab olema füüsiliselt kindel (st perimeetris ei tohi olla tühemikke ega hõlpsat sissemurdmist võimaldavaid alasid). Territooriumi välisseinad peavad olema tugeva ehitusega ja kõik välisuksed peavad olema volitamatu sissepääsu eest sobivalt kaitstud, näiteks reguleerimismehhanismide, riivide, valvesignalisatsiooni, lukkudega jne.

Volitamata sisenemise ja (näiteks kahjutule või üleujutuse põhjustatud) keskkonna saastamise vältimiseks peavad füüsilised tõkked ulatuma aluspõrandast kapitaalse

vahelaeni. Kõik tulekindlad uksed turvaperimeetril peavad olema varustatud valvesignalisatsiooniga ja iselukustuvad.

Füüsiline sissepääs turvaala territooriumile või hoonesse peab olema piiratud, andes pääsu ainult volitatud personalile. Volitatud isiku turvalisel alal viibimine peab olema tagantjärgi tuvastatav.

Turvaliste alade külastajad peavad olema järelevalve all või eelnevalt kontrollitud. Neile tuleb anda sissepääs ainult konkreetseks volitatud otstarbeks ning neile tuleb anda juhised ala turvanõuete ja hädaprotseduuride kohta. Nend viibimine turvalisel alal peab olema tagantjärgi kontrollitav.

Turvalistele aladele pääsuõigusi tuleb perioodiliselt läbi vaadata ja ajakohastada.

5.2.4. Ruumide ja sisseseade turve

Turvaline ala peab olema lukustatud või paiknema lukustatud hooneosas. Turvalise ala valimisel ja kujundamisel tuleb arvestada kahjustuse võimalikkust kahjutule, üleujutuse, plahvatuse, rahutuste ning muude looduslike või tehislike õnnetuste tõttu. Kaaluda tuleb ka turvaohte naaberruumidest.

Arvestada tuleb järgmisi meetmeid:

- Kriitilised vahendid tuleb paigutada nii, et avalik juurdepääs neile oleks välditud.
- Uksed ja aknad peavad inimeste äraolekul olema lukustatud.
- Ladustamiskeskkonnas ning majutaja keskkonnas peab kõiki välisuksi ja juurdepääsuga aknaid hõlmama vastava ala standardite kohaselt paigaldatud ja regulaarselt testitav valvesignalisatsiooni süsteem. E-hääletamise protseduuride läbiviimise ajal tuleb kasutada turvalise ala videovalvet.
- Ohtlikud või kergestisüttivad materjalid tuleb turvaliselt ladustada ohutul kaugusel turvalisest alast. Hulgivarusid, näiteks kirjatarbeid, ei tohi ladustada turvalisel alal. Tulekahju võimaluse vähendamiseks tuleb vältida tuleohtlike materjalide (näiteks pakkematerjalid, varumööbel) hoidmist e-hääletamise süsteemi turvalisel alal.
- Varuandmekandjad tuleb paigutada ohutule kaugusele, et vältida nende kahjustusi õnnetuse korral põhiasukohas.
- Hoones osutatavad teenuste, näiteks koristus-, turva-, remondi ja muude teenuste osutamiseks tuleb sõlmida lepingud, mis tagavad e-hääletamise süsteemi ja selle andmete kaitse teeninduspersonali volitamatute või hooletute tegevuste eest.
- Turvalist ala sisaldavate hoonete ja infrastruktuuri plaanid, sealhulgas evakuatsiooniplaanid, peavad olema uuendatud, kättesaadavad ning nende asukoht peab olema personalile teada.

5.2.5. Seifide turve

Seifide puhul tuleb arvestada kõiki käesolevas dokumendis toodud nõudeid, muuhulgas järgmist:

- Seifi haldava asutuse regulatsioonis on sätestatud seifi võtmete haldajad, võtmete arv ja nende asukoht.
- Seifi võtmed antakse üle allakirjutatud akti alusel, kus on kirjas vastutus ja tagastamise tingimused. Võtme tagastamisel vormistatakse allakirjutatud akt.
- Kui seifil kasutatakse juurdepääsu koode, toimub see vastavalt paroolide halduse reeglitele (arvestades seifi parooli halduse spetsiifikat, näiteks pikkuse ja kasutatavate sümbolite osas).
- Iga hetk on olemas ülevaade isikutest, kes omavad juurdepääsu seifile.

5.2.6. Töö turvalisel alal

Turvalisuse tõstmiseks turvalisel alal tuleb arvestada järgnevat:

- Kõik turvalisel alal tehtavad toimingud tuleb salvestada.
- Järelevalveta tööd turvalisel alal tuleb vältida nii ohutuse kui ka turvalisuse tõttu ning kahjurlike tegevuste võimaluste vältimiseks.
- Tühi turvaline ala peab olema füüsiliselt lukustatud ja seda tuleb perioodiliselt kontrollida.
- Kolmandate osaliste tugiteenuste personalile tuleb anda piiratud juurdepääs turvalistele aladele või tundliku informatsiooni töötluse vahenditele ja ainult vajaduse korral. Sellist juurdepääsu tuleb jälgida.
- Ei tohi lubada volitamata foto-, video-, heli- või muud salvestusaparatuuri.

5.2.7. Saadetiste vastuvõtt

Saadetiste vastuvõtuala tuleb e-hääletamise süsteemist isoleerida volitamatu juurdepääsu vältimiseks. Arvestada tuleb järgnevat:

- Vastuvõtu ala tuleb kujundada nii, et saadetisi saaks üle anda, ilma et kohaletoimetuspersonal pääseks hoone muudesse osadesse.
- Kui sisemine uks on avatud, peavad hoone välisuksed olema turvaliselt suletud.
- Sissetulev materjal tuleb enne ta üleviimist vastuvõtu alalt kasutuskohta üle vaadata võimalike ohtude avastamiseks.

5.2.8. Seadmestiku paigutus ja kaitse

E-hääletamise seadmestik tuleb paigutada, vähendades keskkonnaohtudest tulenevaid riske ja volitamatu juurdepääsu võimalusi. Arvestada tuleb järgnevat:

- Seadmestik tuleb paigutada nii, et tarbetu juurdepääs tööaladele oleks minimaalne.
- Tundlikke andmeid käitlevad infotöötluse ja -talletuse vahendid tuleb paigutada nii, et andmelekke risk nende kasutamise ajal oleks minimaalne.
- Üldise vajaliku kaitsetaseme alandamiseks tuleb salajased andmed ja neid töötlevad seadmed isoleerida.

- Tuleb rakendada meetmeid selliste riskide minimeerimiseks, mille tekitavad potentsiaalsed ohud, sealhulgas vargus, kahjutuli, lõhkeained, suits, vesi (või veevarustuse rike), tolm, vibratsioon, keemilised mõjurid, elektritoitehäired, elektromagnetiline kiirgus.
- Söömine, joomine ja suitsetamine e-hääletamise süsteemi seadmete läheduses on keelatud.
- Arvestada tuleb lähialadel asetleidvate õnnetuste toimet, näiteks kahjutuld naaberhoones, vee leket katuselt maa-alustele korrustele või plahvatust tänaval.

5.3. Loogiline pääsu reguleerimine

5.3.1. Paroolide haldus

Paroolide halduses lähtutakse ISKE M2.11 ja HS.56 nõuetest.

Paroolide varundusel lähtutakse ISKE M2.22 nõuetest, millest lähtuvalt volitamata isikute juurdepääs deponeeritud paroolidele peab olema välistatud. Kui tekib olukord, kus mõnda deponeeritud parooli on tarvis kasutada, peab see toimuma nn nelja silma printsiibil, st kahe inimese poolt korraga. Iga võimaliku deponeeritud parooli kasutamine tuleb dokumenteerida.

HSM füüsilised võtmed antakse üle allakirjutatud akti alusel, kus on kirjas vastutus ja tagastamise tingimused. Üks komplekt HSM operaatorite füüsilisi võtmeid (sinine, punane ja must) varundatakse sarnaselt paroolidega. Valimiskomisjoni liikmete füüsilistest võtmetest (rohelistest) varukoopiaid ei tehta.

5.3.2. Võtmete haldus

E-hääletamise süsteemis kasutatakse viite (süsteemi, HES ja valimiste kodulehe TLS serverite, valijarakenduse ja kontrollrakenduste koodi signeerimise) privaatvõtit. Nende haldamise põhimõtted on toodud jaotises 10.

Süsteemi privaatvõtmega seotud lisaprotseduurid (võtmepaari genereerimine, salajase võtme haldamine, sertifikaadi hankimine, kasutusele võtmine ja turvaline kustutamine) on kirjeldatud dokumendis "Raudvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhis".

6. E-hääletamise põhiandmete turve

6.1. Sissejuhatus

Informatsiooni ja andmekandjate turbe eesmärk on vältida e-hääletamise süsteemi tervikluse kadu, konfidentsiaalsete andmete lekkeid ja tegevuskatkestusi. Infokandjaid tuleb hallata ja füüsiliselt kaitsta.

6.2. Informatsiooni turve

6.2.1. E-hääletajate signeeritud ning krüpteeritud häälte haldamine

E-hääletajate allkirjastatud ning krüpteeritud häälte haldamisel tuleb arvestada järgmist:

1. E-häälte kaitsmine hääletaja arvutis, häälteedastamisserveris ja häältetalletamisserveris toimub e-hääletamise dokumentatsioonis, sealhulgas käesolevas infoturbe poliitikas, toodud meetmete rakendamisega.
2. Juurdepääs e-häältele peab olema minimaalne ja vastama protseduurides sätestatud tegevustele.
3. E-hääletajate allkirjastatud ning krüpteeritud hääled salvestatakse (lisaks talletamisele häältetalletamisserveris) selleks, et teha e-häälte varukoopiaid hääletusperioodil. Muul otstarbel salvestamine toimub vaid dokumenteeritud vajaduse ja EHK kirjaliku loa alusel.
4. Varukoopiate tegemise sagedus e-hääletamise ajal on 1 kord päevas.
   4.1. Varukoopiate tegemine toimub käsitsi. Salvestusmeediana kasutatakse mobiilseid, ühekordselt kirjutatavaid andmekandjaid.
   4.2. Varukoopiate tegemine toimub üldjuhul keset päeva ca 16:00.
   4.3. E-hääletamise viimasel päeval tehakse lõplik varukoopia vahetult peale hääletamisperioodi lõpetamist.
5. Käsitsi varundatud koopiad märgistatakse järgnevalt: märge "E-hääled", salvestamise kuupäev ja kellaaeg.
6. Koopiad mobiilsel andmekandjal säilitatakse seifis.
7. Kõik tegevused e-häältega registreeritakse logis vastavalt salajaste andmete logimise nõuetele.
8. Pärast ebavajalikuks muutumist (üks kuu pärast valimisi või pärast kaebuste menetluse lõppu) hävitatakse e-hääletajate poolt signeeritud ning krüpteeritud häälte kõik koopiad kõigilt seadmetelt turvalise kustutamise või andmekandjate füüsilise hävitamise teel.
9. Häälte kokkulugemise ja kustutamise, vajadusel ka muude protseduuride toimumise faktid dokumenteeritakse vastavalt e-hääletamise protseduuride kirjelduses ettenähtule.

6.2.2. Süsteemi salajase võtme haldamine

Süsteemi salajase võtme haldamisel tuleb arvestada järgmist:

1. Salajase võtme genereerimine, partitsiooni varundamine, salajase võtme hävitamine ning teised tegevused salajase võtmega toimuvad e-hääletamise süsteemi dokumentatsiooni, sealhulgas juhendi "Riistvaralise turvaserveri SafeNet Luna SA haldusjuhend. Tegevusjuhis" ning e-hääletamise käsiraamatu põhjal.
2. Juurdepääs salajasele võtmele peab olema minimaalne ja vastama protseduurides sätestatud tegevustele.
3. Salajase võtme kaitsmine turvamoodulis ja häältelugemisrakenduses toimub käesolevas infoturbe poliitikas toodud kõikide meetmete rakendamisega.
4. Salajast võtit varundatakse ainult spetsiaalsele Luna SA varundustokenile (vt dokument "Raudvaralise turvaserveri SafeNet Luna SA haldusjuhend. Üldosa"), mitte mobiilsele andmekandjale. Varundustokenit hoitakse seifis eraldi riistvaralisest turvamoodulist.
5. Varundustoken pakitakse, märgistatakse ja pitseeritakse.
6. Kõik tegevused varundustokeniga registreeritakse logis vastavalt salajaste andmete logimise nõuetele.
7. Pärast ebavajalikuks muutumist hävitatakse salajane võti turvamoodulist ja varundustokenilt vastavalt HSM ja süsteemiülema juhenditele ja teistele dokumentidele.
8. Salajase võtme genereerimise, partitsiooni varundamise, salajase võtme hävitamise, vajadusel ka muude protseduuride toimumise faktid dokumenteeritakse vastavalt e-hääletamise protseduuride kirjelduses ettenähtule.

6.2.3. Konfidentsiaalse informatsiooni haldamine

Konfidentsiaalse informatsiooni haldamisel tuleb arvestada järgmist:

1. Konfidentsiaalse informatsiooni kaitsmine e-hääletamise süsteemis toimub käesolevas infoturbe poliitikas toodud meetmete rakendamisega.
2. Konfidentsiaalsele informatsioonile tuleb võimaldada minimaalne juurdepääs vastavalt protseduurides sätestatud tegevustele.
3. Kõik koopiad registreeritakse. Koopiad mobiilsel andmekandjal säilitatakse seifis.
4. Pärast ebavajalikuks muutumist hävitatakse konfidentsiaalsed andmed turvalise kustutamise või andmekandjate füüsilise hävitamise teel.
5. Konfidentsiaalse informatsiooni töötlemise protseduuride toimumise faktid dokumenteeritakse vastavalt e-hääletamise protseduuride kirjelduses ettenähtule.

Vastavalt ülalmainitud põhimõtetele toimub ka valimiste veebisaidi TLS serveri ja valijarakenduse koodi signeerimise võtmepaaride salajaste võtmete haldamine.

6.2.4. Kriitilise informatsiooni haldamine

Tervikluse seisukohast kriitilise, kuid mitte konfidentsiaalse informatsiooni haldamisel tuleb silmas pidada järgmist:

- Andmete kaitse toimub käesolevas infoturbe poliitikas toodud meetmete rakendamisega.
- Juurdepääs kriitilistele andmetele peab olema minimaalne ja vastama protseduurides sätestatud tegevustele
- Kriitilistest andmetest tehakse vaid protseduurides sätestatud vajalikke koopiaid. Koopiate loomise faktid dokumenteeritakse vastavalt e-hääletamise protseduuride kirjelduses ettenähtule.
- Selliste andmete töötlusel fikseeritakse andmete tervikluse seisukohast olulised koopiad (esmased koopiad) ning jälgitakse, et nende terviklus oleks tagatud.
- Esmased koopiad märgistatakse järgnevalt: andmete nimetus, versioon (vajadusel), autor või väljaandja, loomise kuupäev ja kellaaeg. Dokumentide kohta võib esitada ka muid rekvisiite vastavalt juhendile "E-hääletamise dokumentatsioon".
- Esmased koopiad säilitatakse seifis.
- Kõik tegevused esmaste koopiatega registreeritakse logis vastavalt kriitiliste andmetega sooritatud tegevuste logimise nõuetele.
- Pärast ebavajalikuks muutumist hävitatakse kriitilise informatsiooni koopiad turvalise kustutamise või andmekandja füüsilise hävitamise teel.

6.3. Mobiilsete andmekandjate turve, haldamine ja kõrvaldamine

Mobiilse andmekandjana on kasutusel ainult irdmeedia (DVD plaadid, USB-kõvakettad, välksalvestid (flash-memory), USB-mälupulgad) ja paber (prinditud aruanded, dokumentatsioon jne). Salajasi andmeid transporditakse võimalusel irdmeediaga. Kõik tegevused konfidentsiaalseid või kriitilisi andmeid kandvate mobiilsete andmekandjatega (andmekandja initsialiseerimine; andmete salvestamine, kasutamine, muutmine, kustutamine; andmekandja hävitamine jne) registreeritakse vastavalt logimise nõuetele.

Kõik andmekandjad, milledele salvestatakse konfidentsiaalset või kriitilist informatsiooni, tuleb märgistada sisu näitava märgistusega.

Väliste andmekandjate haldamisel tuleb arvestada järgmist:

- Mobiilsete andmekandjate kaitse toimub käesolevas infoturbe poliitikas toodud meetmete rakendamisega.
- Kõiki infokandjaid tuleb säilitada ohutus turvalises keskkonnas (näiteks seifis) ja kooskõlas valmistaja tehniliste tingimustega.

- Kui ükskõik millise organisatsioonist kõrvaldamisele kuuluva korduvkasutusega infokandja sisu pole enam vajalik, tuleb ta kustutada.
- Kõigi infokandjate kõrvaldamine organisatsioonist peab olema volitatud, kõigi selliste kõrvaldamiste kohta tuleb säilitada jälg logis.

Andmevahetuseks kasutatavaid mobiilseid andmekandjaid (USB-kõvakettad või välksalvestid (flash-memory) nagu USB-mälupulgad) ei tohi kasutada teiste andmete transpordiks ega hoiustamiseks. Mobiilsed andmekandjad tuleb tähistada, et ei toimuks nende ekslikku kasutamist muude funktsioonide täitmiseks.

7. Turvalisust toetavad töösisekorra eeskirjad

7.1. Ründetarkvara tõrje

Ründetarkvara võib põhjustada konfidentsiaalsete andmete avalikustamist, andmete tervikluse kadu ja muid soovimatuid tagajärgi. Ründekoodi eest kaitsmiseks tuleb rakendada järgmisi meetmeid:

- baastarkvara ja uuenduste laadimine ainult usaldusväärsest ja kontrollitud allikast,
- tarkvara turvauuenduste pidev paigaldamine,
- tulemüüride kasutamine,
- võrguühenduste ja mobiilsete andmekandjate kasutamise kitsendamine vaid süsteemi protseduurides ette nähtud juhtudeni, igasugune muu võrguühenduste ja mobiilsete andmekandjate kasutamine on keelatud,
- viiruste ja nuhkvara skännerite kasutamine,
- tervikluse kontroll,
- andmeallikate sertifitseerimine ja kontroll,
- teavitamine ja koolitus.

7.2. Kaugtöö

Kaugtööks kasutatakse sidetehnikat, mis võimaldab personalil töötada e-hääletamise süsteemi vahenditega väljaspool oma organisatsiooni asuvas püsivas kaugasukohas.

E-hääletamise kesksüsteem on varustatud kaugseire vahenditega, mis võimaldavad süsteemi põhiparameetreid ja statistilisi näitajaid turvaliselt üle võrgu jälgida. Muud laadi kaugtöö ei ole e-hääletamise kesksüsteemis lubatud (e-hääletamist ei loeta kaugtööks).

Valimiste kodulehe haldus ja valija- ning kontrollirakenduse avaldamine toimub kaugtöö abil vastavalt keskkonna kasutusjuhendile.

Kaugtöö käigus töödeldava informatsiooni turvalise käitlemise eest vastutab kaugtöö teostaja.

7.3. Tühja laua ja tühja ekraani poliitika

Informatsioonile volitamatu juurdepääsu, informatsiooni kaotuse ja kahjustuse riskide vähendamiseks tuleb turvalistel aladel rakendada tühja laua poliitikat paberdokumentide ja mobiilsete salvestuskandjate puhul ning tühja ekraani poliitikat infotöötlusvahendite puhul, nii normaalsel tööajal kui väljaspool seda.

8. Side ja võrguhalduse turve

Andmeid kandev või IT-teenuseid toetav toite- ja sidekaabeldus tuleb kaitsta andmepüügi, kahjustuste ja ülekoormuse eest. Kaabeldus tuleb füüsiliselt kaitsta juhuslike või sihilike kahjustuste eest.

Võrguhalduse turvameetmed on järgmised:

- Võrkude õige ja turvalise töö tagamiseks on kehtestatud ja dokumenteeritud ekspluatatsiooniprotseduurid ja vastutused. Jälgitakse turvaintsidentidele reageerimise protseduuri.
- Võrgu usaldatavaks talitluseks on oluline ta sobiv infrastruktuur ja konfigureerimine. See hõlmab muuhulgas standardset serverite konfigureerimise metoodikat ja head dokumenteerimist. Eriotstarbelisi servereid tuleb kasutada ainult määratud otstarveteks.
- Muudatused võrgu koosseisus plaanitakse, dokumenteeritakse, kinnitatakse, nende mõju analüüsitakse ja neid hallatakse vastavalt konfiguratsioonihalduse põhimõtetele.
- Riskide ja väärkasutuse võimaluste minimeerimiseks töötavas võrgus tuleb hoida loogiliselt ja füüsiliselt lahus kriitiliste tööalaste tegevuste ja andmetega seotud alad. Samuti tuleb arendusvahendid hoida lahus ekspluatatsioonivahenditest.
- Usaldatava talitluse ning võrgu adekvaatse läbilaskevõime tagamiseks on vajalik ennetav plaanimine ja ettevalmistus, samuti seire (mis hõlmaks koormuse statistikat). Nõrkuste tuvastamiseks tuleb kasutada võrgu seiret, mis aitab tuvastada ründajaid.
- Katsed pääseda e-hääletamise süsteemi ja edukad lubamatud sisenemised tuleb avastada ja dokumenteerida, et neile asjakohaselt ja toimivalt reageerida.

Et vähendada võrkudest tulenevaid riske, on võrguhalduse turbe põhimõte "kõik, mis pole e-hääletamise protseduuride läbiviimiseks otseselt vajalik, on keelatud", täpsemalt:

- Arvutite omavahelised ühendused on minimeeritud ainult otseselt vajalikele ülesannetele vastavaks.
- Ühendused Internetiga on minimeeritud ainult otseselt vajalikele ülesannetele vastavaks.
- E-hääletamise süsteem on kaitstud eraldi tulemüüriga. Võrguühenduse ja tulemüüri konfiguratsioonid lubavad ainult spetsifitseeritud tegevusi, võimalusel kitsendades IP-aadressid, protokollid ja pordid.
- Teenused ja tegevused on minimeeritud ainult otseselt vajalikele ülesannetele vastavaks.

E-hääletamise süsteemi arvutivõrgu ülesehitus ja Interneti ühendused on kirjeldatud dokumendis "E-hääletamise organisatsioon ja infrastruktuur".

E-hääletamise arvutitele baassüsteemide paigaldamisel, operatsioonisüsteemide turvapaikade laadimisel ja muude teenindusprotseduuride käigus kasutatakse

soovitatavalt mobiilseid andmekandjaid (USB-kõvakettad või välksalvestid (flash-memory), USB-mälupulgad).

E-hääletamise süsteemiga seotud teabevahetuse turvamiseks tuleb kasutada digitaalselt allkirjastatud faile või krüpteerimist.

9. Infrastruktuuri turve

9.1. Varutoiteallikad

Seadmed tuleb kaitsta toitekatkestuste ja muude elektriliste anomaaliate eest. Kasutada tuleb seadme tootja tehnilistele tingimustele vastavat sobivat elektritoiteallikat. Toite pidevuse saavutamiseks e-hääletamise perioodil kasutatakse vähemalt kahte järgmistest võimalustest:

- mitu toiteliini kriitilise tõrkepunkti vältimiseks toitesüsteemis,
- puhvertoiteallikas (UPS),
- varugeneraator.

UPS peab toite katkestuse korral tagama HES ja HTS normaalse töö vähemalt ühe ööpäeva jooksul. Ootamatuseplaanid peavad hõlmama meetmeid UPS-i tõrke puhuks. Adekvaatse töövõime tagamiseks tuleb UPS-i riistvara regulaarselt kontrollida ja testida teda vastavalt valmistaja soovitustele.

Kui kasutatakse varugeneraatorit, tuleb seda regulaarselt testida vastavalt valmistaja juhistele. Generaatori pikemaajalise töö tagamiseks peab kasutada olema asjakohane kütusevaru.

Peale selle peaksid riistvararuumide hädaväljapääsude läheduses asuma avarii-toitelülitid toite kiire väljalülituse hõlbustamiseks avarii korral. Võrgutoite katkemise puhuks tuleb tagada avariivalgustus. Hoone peab olema kaitstud pikse vastu, välised sideliinid tuleb vajadusel varustada piksefiltritega.

9.2. Kaabelduse turve

Andmeid või tugiinfoteenuseid kandev jõu- ja sidekaabeldus tuleb kaitsta andmepüügi ja kahjustuste eest. Tuleb rakendada järgmisi meetmeid:

- Infotöötlusvahendite juurde kulgevad toite- ja sideliinid peaksid olema adekvaatselt kaitstud.
- Võrgukaabeldus tuleb kaitsta volitamatu andmepüügi ja kahjustuste eest, näiteks kaitsekanalite kasutamisega või vältides läbi avalike alade kulgevaid marsruute.
- Häiringute vältimiseks tuleb jõukaablid eraldada sidekaablitest.
- Ruumide või jaotuskarpide lukustamine kontroll- ja lõpp-punktides.
- Kahtluse korral pealtkuuldeotsingu algatamine kaablitele ühendatud volitamata seadmete leidmiseks.

Kuna töödeldavad andmed kuuluvad H turvaklassi, siis rakenduvad H turvaklassist tulenevad lisanõuded HG.64 "Lisanõuded kaabelduse dokumenteerimisele ja märgistusele", HS.47 "Lisanõuded tarbetute liinide kõrvaldamisele" ja HS.48 "Kõrgkonfidentsiaalsuse lisanõuded IT kaabelduse paigaldusele".

9.3. Seadmestiku hooldus

Pideva käideldavuse ja tervikluse tagamiseks tuleb seadmeid õigesti hooldada. Arvestada tuleb järgmist:

- Seadmeid tuleb hooldada vastavalt valmistaja soovitatud hooldusintervallidele ja tehnilistele tingimustele.
- Seadmeid peab remontima ja hooldama ainult volitatud hooldepersonal.
- Kõik oletatavad või tegelikud tõrked ning kogu profülaktiline ja korrektiivne hooldus tuleb registreerida.
- Seadmete saatmisel hoolduseks väljaspoole territooriumi tuleb rakendada asjakohaseid meetmeid (sealhulgas andmete turvaline kustutus). Järgida tuleb kõiki kindlustuspoliisidest tulenevaid nõudeid.

9.4. Seadmete turve väljaspool turvalist ala

Tuleb arvestada järgmist:

- E-hääletamise seadmetega ei tehta tööd väljaspool turvalist ala.
- Seadmeid, informatsiooni ega tarkvara ei tohi e-hääletamise süsteemi turvaliselt alalt loata välja viia. Seadmete väljaviimine ja tagasitoomine tuleb registreerida.
- Turvaliselt alalt väljaviidud seadmeid ja infokandjaid ei tohi jätta avalikes kohtades järelevalveta.
- Tuleb jälgida valmistaja juhiseid seadmete kaitse kohta, näiteks tugevatele elektromagnetilistele väljadele avatuse eest kaitsmise kohta.

10. Personali turve

10.1. Sissejuhatus

Personali turvet tuleb rakendada:

- Põhi- ja lepinguliste töötajate puhul – töökohtade ja vastutuste määratlemisel, personali valikul, töölepingute sõlmimisel, töötajate koolitusel, töövahekorra kestel (sealhulgas intsidentide halduses) ning selle lõpetamisel.
- Kolmandate osapoolte puhul – pakkumiskutsetes, hangetes, lepingutes ning tööde teostamisel ja järelevalves.

10.2. Töökohustused ja töölevõtmine

Töökohustustes tuleb dokumenteerida turvarollid ja -kohustused vastavalt organisatsiooni infoturbepoliitikale. Kohustused peavad sisaldama üldist vastutust turvapoliitika evitamise või järgimise eest ning konkreetseid kohustusi e-hääletamise süsteemi kriitiliste varade kaitse ja turbega seotud protsesside või tegevuste sooritamise eest.

Organisatsiooni turvapoliitikaid ja -protseduure oluliselt või korduvalt rikkunud töötajate puhul tehakse ettekanne Vabariigi Valimiskomisjonile, kes algatab vajadusel asja uurimise ja menetluse. Töötajad peavad olema teadlikud IT-süsteemide turvapoliitikate ning muude dokumenteeritud turvalepete tahtliku või tahtmatu rikkumise tagajärgedest.

E-hääletamise organisatsiooni alaline personal on EHK liikmed, kes määratakse ametisse Vabariigi Valimiskomisjoni otsusega.

10.3. Kohustuste lahusus ja roteerimine

Kriitilisi protseduure tuleb läbi viia vaid vähemalt kahe sõltumatu inimese koostöös. Üldjuhul on üks neist kriitilise protseduuri otsene läbiviija ning teine või teised jälgivad seda.

Kriitiliste protseduuride täitjaid tuleb roteerida kahel viisil. Protseduuride otsest läbiviijat tuleb sama grupi raames roteerida (kord viib läbi üks, siis teine).

Lisaks on soovitatav selliste protseduuride läbiviijaid regulaarselt asendada teiste isikutega, näiteks dubleerivate töötajatega. Sellised vahetused võivad toimuda näiteks pärast teatud arvu valimiste läbiviimist.

Niivõrd kui võimalik, täidetakse kriitilisi protseduure väljaspool hääletusperioodi.

10.4. Turvateadlikkus ja -koolitus

Koolituse eesmärk on tagada kasutajate teadlikkus infoturbeohtudest ja -probleemidest ning nende suutlikkus organisatsiooni turvapoliitika toetamiseks oma normaalse töö käigus.

Kõik e-hääletamise süsteemi töötajad ja vajaduse korral kolmandatest osalistest kasutajad peavad läbima asjakohase koolituse ja regulaarse täiendõppe organisatsiooni poliitikate ja protseduuride alal. See hõlmab turvanõudeid, õiguslikke kohustusi ja tööalaseid meetmeid, samuti informatsioonile või teenustele juurdepääsu andmise eelset koolitust infotöötlusvahendite õige kasutamise alal, näiteks sisselogimisprotseduuri, tarkvarapakettide kasutamist.

10.5. Kolmandate osapoolte personal

Kolmandate osapoolte personali (näiteks koristajaid, turvapersonali, riistvara ja tarkvara hooldajaid) tuleb kontrollida või nõuda vastavat kontrolli kolmandalt osapoolelt.

Kolmandate osapoolte personali juurdepääs e-hääletamise süsteemi vahenditele peab põhinema ametlikul lepingul. Lepingusse lülitamiseks tuleb kaaluda järgmisi tingimusi:

1. Üldine infoturbe poliitika
2. Varade kaitse
3. Kättesaadavaks tehtavate vahendite kirjeldus
4. Pääsu reguleerimise lepped, mis hõlmavad:
   4.1. lubatavaid pääsumeetodeid ning üheste identifikaatorite, näiteks kasutajatunnuste ja paroolide reguleerimist ja kasutamist,
   4.2. volitamisprotsessi, millega kasutajaile antakse juurdepääs ja õigused,
   4.3. nõuet pidada nimekirja isikutest, kes on ligipääsuks volitatud ning nende õigustest ja privileegidest.
5. Personali koolitamine meetodite, protseduuride ja turbe alal
6. Õigus jälgida ja peatada kasutaja tegevust
7. Õigus auditeerida lepingulisi kohustusi või lasta selliseid auditeid sooritada kolmandal osalisel
8. Probleemi lahendamise protsessi kehtestamine, sätted ootamatuste puhuks

11. Alltöövõtu poliitika

Alltöövõtu poliitika eesmärk on säilitada e-hääletamise süsteemi turvalisus ka siis, kui infotöötluskohustus on tellitud teiselt organisatsioonilt.

Väljasttellimise korraldus peab pooltevahelises lepingus käsitlema e-hääletamise süsteemi riske, turvameetmeid ja protseduure.

Poolte vahel sõlmitud leping peab käsitlema:

- VVK poolt alltöövõtjale esitatavaid turvanõudeid ning nende täitmiseks kohustuslikus korras rakendatavaid meetmeid,
- VVK õigust nende nõuete täidetust kontrollida,
- Alltöövõtja kohustus intsidentidest teavitada,
- Alltöövõtja vastutust nõuete mittetäitmise korral.

12. Süsteemi muudatuste haldus

E-hääletamise süsteem ja selle talitluskeskkond on pidevas muutumises. Need muutused tulenevad uute funktsioonide ja teenuste kättesaadavusest või uute ohtude ja nõrkuste avastamisest. Need muutused võivad aga põhjustada uusi ohte ja nõrkusi. Süsteemi muutuste hulka kuuluvad:

- tarkvara muudatused,
- dokumentatsiooni muudatused,
- protseduuride muudatused,
- riistvara uuendamine,
- uued kasutajad,
- muudatused võrkude konfiguratsioonis,
- muudatused asukohas või teenusepakkujates.

Kui e-hääletamise süsteemis toimub muutus või kui seda plaanitakse, on oluline kindlaks teha, kas ja kuidas see muutus mõjutab süsteemi turvalisust. Süsteemi infoturbe juht võib vastavad määrangud teha ise (vajadusel koos teenusepakkuja või teiste osapooltega) või volitada sellise analüüsi tegijaks pädevat osapoolt.

Suuremate muutuste korral, mis toovad kaasa uue riistvara, tarkvara või teenuse hankimist, on vajalik analüüs uute turvanõuete määramiseks. Ka väiksemad muudatused võivad kaasa tuua vajaduse mõningaseks analüüsiks.

Muudatuste halduse protseduurid on täpsemalt kirjas dokumendis “E-hääletuse käsiraamat”.

13. Sündmuste logimine

Kõik e-hääletamise süsteemi toimingud logitakse automaatselt või kasutajate poolt.

Automaatselt logitakse vähemalt:

- Edukad ja edutud süsteemi sisselogimise katsed
- Lubamatud andmepöördused
- Eriolukorrad ja rikked
- Tegevused salajaste ja kriitiliste andmetega

Süsteemi kasutajad logivad failis või paberkandjal vähemalt järgmist:

- Regulaarselt teostatud protseduuri nimetus, sooritamise aeg, sooritajad, kontrollijad, tulemused ja kõrvalekalded, kui neid oli.
- Kõik toimingud salajaste andmete ja vastavate andmekandjatega, sealhulgas loomine, kopeerimine, muutmine, kustutamine, hävitamine. Logitakse toimingu sisu, sooritamise aeg, sooritajad, kontrollijad, tulemused ja kõrvalekalded, kui neid oli.
- Kõik ebastandardsed (e-hääletamise protseduurides mitte ette nähtud) toimingud kriitiliste andmetega. Logitakse toimingu otstarve, toimingu sisu, sooritamise aeg, sooritajad, kontrollijad, tulemused ja kõrvalekalded, kui neid oli.

Logid on turvakriitilised andmed (ISKE klass *K1 T2 S2* tase *M*) ja hallatakse vastavalt ISKE nõuetele.

14. Turvaintsidentide haldus

14.1. Intsidendi määratlus

E-hääletamise protseduuride tegevuse katkematuse nõuded on järgnevad:

- E-hääletamine hääletusperioodil, hääletusperioodi protseduurid majutusteenuse pakkuja asukohas – lubatud on üks katkestus päevas maksimaalse pikkusega 15 minutit.
- Muud kriitilised protseduurid katkestus (viivitus) kuni neli tundi, kui protseduuris ei ole sätestatud teisiti.

Järgnevaid olukordi nimetatakse edaspidi kriitilisteks:

- Salajaste andmete tõenäoline leke
- Kriitiliste andmete häving või tõenäoline volitamatu muutmine
- Häired kriitiliste seadmete töös, mis võivad seada kahtluse alla e-hääletamise toimumise või usaldusväärsuse, muuhulgas e-hääletamise protseduuride katkematuse nõuete piiridest väljuvad katkestused.
- Suuremahuline edukas rünne, mille tulemusena võib olla kompromiteeritud suur osa e-hääletajate arvutitest.
- Dokumendis "Toompea lossis viibivate isikute ohuolukorras tegutsemise kord" nimetatud ohuolukorrad
- Infrastruktuuri katkestused majutusteenuse pakkuja juures e-hääletuse perioodil
- Muud olukorrad, mis võivad oluliselt halvendada e-hääletamise süsteemi toimimist või kompromiteerida süsteemi või seda haldavaid organisatsioone (näiteks häired kehtivuskinnituse teenuse osutamisel, suuremahuline konfidentsiaalsete andmete leke jne).
- Muud olukorrad, mille puhul on vaja intsidendist informeerida avalikkust.

Intsidenti, mis tuleneb ülalmainitud olukordadest, nimetatakse edaspidi kriitiliseks intsidendiks.

14.2. Intsidendihalduse üldpõhimõtted

Turvaintsidentide halduse põhimõtteid kirjeldatakse täpsemalt intsidendihaldust käsitlevas eraldi dokumendis “Elektroonilise hääletamise intsidentide haldamise süsteem”.

1. Intsidentidest teatatakse võimalikult kiiresti EHK esimehele, tema kohusetäitjale või täiendavale turvaintsidentide haldajale.
2. Edastatakse kogu olemasolev informatsioon, alustades andmetest, mis on vajalikud intsidendi registreerimiseks turvapäevikusse.

3. Intsidendi kohta käivad asitõendid säilitatakse.
4. EHK esimees määrab intsidendi prioriteedi, sellega tegelejad ning tegelemise viisi.
5. Tõsistest intsidentidest informeeritakse esimesel võimalusel Vabariigi Valimiskomisjoni.
6. Enne ja pärast valimisi tehakse Vabariigi Valimiskomisjonile ülevaade kõikidest turvaintsidentidest.
7. Intsidentide haldamise korda tutvustatakse e-hääletamise süsteemis tegutsevatele isikutele.

15. Varundus ja taaste

Kõigist kriitilistest andmetest tehakse varukoopiad.

Varukoopiaid kasutatakse andmete taastet nõudvate intsidentide halduses. Intsidentide käsitlust on täpsemalt kirjeldatud dokumendis "Elektroonilise hääletamise intsidentide haldamise süsteem."

Varukoopiate alusel taastet tuleb testida, hooldada ja rakendada nii, et ta muutuks kõigi muude haldusprotsesside lahutamatuks osaks.

Enne iga järjekordset e-hääletamist tuleb varundust testida, et veenduda ta toimivuses tegeliku elu tingimustes ja selles, et kõik asjassepuutuvad töötajad tunnevad plaani. Testimiseks simuleeritakse vähemalt kahe erinevat tüüpi kriitilise intsidendi lahendamist.

Salajaste andmete varukoopiate tegemise sagedus ja kandja on määratud eespool salajaste andmete haldamist käsitlevates alajaotistes.

Üldine põhimõte on selline, et võimalusel ei varundata andmeid, mida saab genereerida. Kriitiliste mittesalajaste andmete varukopeerimiste sagedus on järgmine:

- E-hääletamise tarkvara – varundatakse iga muudatuse tegemisel.
- E-hääletamise süsteemi dokumentatsioon – varundatakse iga muudatuse tegemisel.
- Konkreetseks e-hääletamiseks loodud süsteemi olekupuu – varundatakse kiireks taastamiseks kohe pärast loomist koos häälestusandmetega.
- Kandidaatide nimekiri – varundatakse hankimisel.
- Valijarakendus – varundatakse iga muudatuse tegemisel.
- Süsteemi võtmepaar – vt salajase võtme haldamisprotseduur.
- E-hääletajate poolt signeeritud ning krüpteeritud hääled – vt jaotis "E-hääletajate poolt signeeritud ning krüpteeritud häälte haldamine".
- Krüpteeritud, signeerimata hääled – ei varundata, luuakse vajadusel iga kord uuesti.
- E-hääletajate digitaalallkirjadest tuletatud hääletajate andmed – ei varundata, luuakse vajadusel iga kord uuesti.
- E-hääletanute nimekirjad jaoskondadele – ei varundata, luuakse vajadusel iga kord uuesti.
- Komisjonide tühistusavaldused – tekib Valimiste infosüsteemi ja varundatakse seal vastavalt vajadusele.
- VVK tühistamise ennistamisavaldused – tekib Valimiste infosüsteemi ja varundatakse seal vastavalt vajadusele.
- Hääletustulemused – ei varundata, luuakse vajadusel iga kord uuesti.
- Logid – varundatakse sama sagedusega nagu e-hääletajate poolt signeeritud ning krüpteeritud hääled.

Varukoopiad tuleb turvaliselt ladustada kaugemal originaalandmekandjatest ning regulaarselt kontrollida taaste usaldatavust.

16. Mittevajalike andmete, seadmete ja liinide hävitamine

16.1. Täielik kustutus

Salajase informatsiooni konfidentsiaalsus tuleb säilitada ka siis, kui seda enam ei vajata. Tuleb tagada, et konfidentsiaalset materjali sisaldavad failid kustutatakse ja kirjutatakse füüsiliselt üle või hävitataks muul viisil. Täielikuks ja turvaliseks kustutuseks peavad kasutajate käsutuses olema infoturbe juhi kinnitatud vahendid. Eriti tuleb hoolitseda mobiilsete andmekandjate eest (USB-kõvakettad või välksalvestid (flash-memory), USB-mälupulgad).

16.2. Seadmete turvaline hävitamine ja taaskasutus

Salajast informatsioon võidakse paljastada seadmete hooletu kõrvaldamise või taaskasutusega. Tundlikku informatsiooni sisaldavad mäluseadmed tuleb tavalise kustutusfunktsiooni kasutamise asemel füüsiliselt hävitada või turvaliselt üle kirjutada.

Seadmed, mis sisaldavad salvestuskandjaid, näiteks kõvakettaid, tuleb kontrollida veendumiseks, et enne seadme kõrvaldamist on kõrvaldatud või üle kirjutatud kõik tundlikud andmed ja kogu litsentsitud tarkvara. Tundlikke andmeid sisaldavate kahjustatud mäluseadmete puhul võib olla vajalik riski hindamine otsustamiseks, kas seade tuleb hävitada, remontida või kõrvaldada.

16.3. Tarbetute liinide kõrvaldamine

Vastavalt ISKE HS.47 "Lisanõuded tarbetute liinide kõrvaldamisele" kõrvaldatakse mittevajalikud sideliinid.

LISA A. Infovarad ja nende turvavajadused

Andmed

1. Tabel: Andmete turvaklassid

Turvaklass	Infovara	Kommentaar
K2 T1 S2 (M)	Hääletamistulemus	Erandlik infovara, mis liigub klassist S2 klassi S0 valimispäeval kell 20:00. (EP valimistel 23:00)
K1 T1 S0 (M)	E-hääletamise kesksüsteemi ja kontrollirakenduse tarkvara lähtekood	HES, HTS, HLR, AR lähtekoodide ja seadistuste avalik osa, kontrollirakenduste lähtekoodid
K1 T1 S2 (M)	E-hääletamise tarkvara lähtekood	Valijarakendus, kesksüsteemi turvaseaded ja ründetuvastustarkvara, keskserverite kettatõmmised. NDA nõue nõrgalt reguleeritud seaduse tasemel
K1 T1 S0 (L)	E-hääletamise tugitarkvara	Baas-operatsioonisüsteemid, HSM tarkvara.
K1 T2 S0 (M)	Hääletamissüsteemi avalik seadistus	Vt allpool Kuna tervikluse rikkumine võimaldab hääletamistulemuse tervikluse rikkumist, siis on nõue kõrgem.
K1 T2 S2 (M)	Hääletamissüsteemis käideldavad isikuandmeid sisaldavad andmed	Vt allpool Saab teada inimese nime ja isikukoodi, mis kell ta hääletas, kui mitu korda ja kas hääl tühistati või läks arvesse.

Turvaklass	Infovara	Kommentaar
K1 T2 S2 (M)	Hääletamissaladuse rikkumist kaudselt võimaldavad andmed	Vt allpool Kui need andmed satuvad kellegi kätte, siis teatud teiste tingimuste täidetud olemisel saab see keegi teada, kes kuidas hääletas.
K1T3S3 (H(HT HS))	Hääled ja lugemisvõtmed	Hääletamistulemuse korrektse selgumise ja salajasuse säilimise seisukohast kriitilised andmed
K1T3S3 (H(HT HS))	Muud privaatvõtmed	HES ja valimiste kodulehe TLS serveri privaatvõtmed, valija- ning kontrollirakenduste signeerimise privaatvõti. Nende andmete avalikuks saamisel on võimalik moonutada hääletustulemust või saada teada hääletussaladuse rikkumist kaudselt võimaldavaid andmeid, samuti rünnata valijate seadmeid.
K0T0S0	Anonümiseeritud ja pseudonümiseeritud logid	E-hääletamise lõppedes hilisemate teadustööde või muude statistiliste uuringute tarbeks tehtavad koopiad logidest, kust on eemaldatud isikuandmed

Hääletamissüsteemi avalik seadistus

- Kandidaatide nimekiri
- Ringkondade-/jaoskondade nimekiri
- Kandidaatide, ringkondade, jaoskondade, valijate ja tühistusnimekirjade autentsust ja terviklust tõestav sertifikaat
- Sertifikaatide konfiguratsioon
- HES sertifikaat
- Pakendatud valijarakendus
- Valimiste veebileht

- Valijarakenduse terviklust tõestav informatsioon
- Autentse valijarakenduseni juhatav informatsioon
- Elektroonilise hääletamise avalik võti
- Valijarakenduse seadistus
- Pakendatud kontrollirakendused

Hääletamissüsteemis käideldavad isikuandmeid sisaldavad andmed

- Algne valijate nimekiri
- Valijate nimekirjade täiendused
- Elektrooniliselt hääletanute nimekiri
- Elektrooniliste häälte tühistusnimekiri
- Serverite logid
- LOG1
- LOG2
- LOG3

Hääletamissaladuse rikkumist kaudselt võimaldavad andmed

- LOG1 – LOG5 üheskoos
- HES privaatvõti
- Allkirjastatud ja krüpteeritud hääled
- Keskserverite võrguliikluse salvestused

Hääled ja lugemisvõtmed

- HSM administraatori parool
- Partitsiooni parool
- HSM operaatorivõtmed (sinised, punased, mustad) ja PIN-koodid
- Elektroonilise hääletamise privaatvõtme aktiveerimise võtmed (rohelised)
- Anonümiseeritud hääled
- Elektroonilise hääletamise privaatvõti

Riistvara

Moodulid	Turvaklass	Infovara	Kommentaar
B3.101 Server, B3.102 Server Unixi all, B3.301 Turvalüüs (tulemüür), B5.2 Andmekandjatel toimuv andmevahetus, B2.12 IT kaabeldus B2.2 Elektrotehniline kaabeldus	K1 T2 S2 (M)	Kesksüsteemi tööriistvara	Kesksüsteemi tööriistvara (majutatud teenusepakkuja juures), HES, HTS, veebiserver, tulemüür, irdmeedia seadistuste liigutamiseks.
B3.102 Server Unixi all, B3.202 Autonoomne IT-süsteem, B5.2 Andmekandjatel toimuv andmevahetus, B2.12 IT kaabeldus B2.2 Elektrotehniline kaabeldus	K2 T3 S3 (H(HT, HS))	Häältelugemise riistvara	HSM, HLR, HTS lugemisperioodil, hääletamistulemuse allkirjastamise ja laadimise tööjaam, auditirakenduse käitamine, irdmeedia tulemuse liigutamiseks
B3.202 Autonoomne IT-süsteem, B3.204 Klient Unixi all või B3.210 Klient Windows Vista all (otsi värkemaid nõudeid) B3.203 Sülearvuti? B5.2 Andmekandjatel toimuv andmevahetus	K1 T2 S2	Kesksüsteemi tugiriistvara	Kesksüsteemi ja valijarakenduse valmendamise tööjaamad. Paikade ja nimekirjade laadimise tööjaamad. Tühistusnimekirjade loomise tööjaam. Irdmeedia seadistuste ja paikade transpordiks.
B 3.203 Sülearvuti	K0 T0 S2	Administraatori arvuti	Logide vaatamiseks, turvaklass sama, mis logidel

Moodulid	Turvaklass	Infovara	Kommentaar
B3.406 Printerid , koopiamasinad ja muud multifunktsionaalsed seadmed, B3.202 Autonoomne IT-süsteem	K1 T1 S2	Printer	E-hääletanute nimekirja trükkimine