Nõuded salastatud teabe töötlussüsteemile

Nr	Nõude kirjeldus	Süsteemis töödeldava teabe kõrgeim salastatuse tase	
		K/S/TS	P
Töötlussüsteemide üldnõuded			
Identimine ja autentimine			
1.	Peetakse nimekirja süsteemi kõigist volitatud kasutajatest.	Jah	Jah
2.	Süsteemi igal volitatud kasutajal on isikustatud kasutajakonto. Süsteemile juurdepääsuks kasutatakse unikaalset kasutajatunnust ja salasõna või Välisluureameti heakskiidetud muid meetodeid.	Jah	Jah
3.	Süsteemi kasutajatele kasutusõiguste andmise, muutmise ja lõpetamise üle peetakse arvestust. Kasutaja kasutusõiguste lõpetamisel kasutajakontot ei kustutata, vaid desaktiveeritakse esimesel võimalusel.	Jah	Jah
4.	Salasõna süsteemile juurdepääsuks on teada üksnes kasutajale.	Jah	Jah
5.	Salasõnal on miinimumpikkus.	Jah, 15 tähemärki	Jah, 15 tähemärki
6.	Salasõnal on maksimaalne kehtivusaeg.	Jah, üks aasta	Jah, üks aasta
7.	Salasõnal on minimaalne kehtivusaeg.	Jah, üks päev	Jah, üks päev
8.	Salasõnas peab sisalduma järgnevast neljast tingimusest kolm: suur täht, väike täht, erimärk, number.	Jah	Jah
9.	Kergesti ära arvatavad salasõnad või kombinatsioonid on keelatud.	Jah	Jah
10.	15 varem kasutuses olnud salasõna kasutamine on keelatud.	Jah	Jah
11.	Salasõnade ristkasutus eri töötlussüsteemide vahel on keelatud.	Jah	Jah
12.	Salasõna muudetakse viivitamata süsteemi intsidendi või salasõna volitamata isikute valdusse sattumise või sellekohase kahtluse ning esmase salasõna korral.	Jah	Jah
13.	Salasõna võib säilitada hoiukohas, mis vastab vastava tasemega salastatud teabekandjate hoiukohale seatud tingimustele, või Välisluureameti kooskõlastatud krüpteerimismeetodiga krüpteeritult. Kui salasõnu säilitatakse ühiskasutuses olevas hoiukohas või turvaala avatud hoiualal, mis vastab vastava tasemega salastatud teabekandjate hoiukohale seatud tingimustele, siis hoitakse neid suletud läbipaistmatus ja juurdepääsuvajaduseta	Jah	Jah

	isikute poolt avamist tuvastada võimaldavas ümbrises.		
14.	Süsteemi haldamisega seotud isikustamata administraatorikonto kasutajatunnust, salasõna ja muud autentimiseks vajalikku teavet tuleb säilitada suletud läbipaistmatus ja volitamata isikute poolt avamist tuvastada võimaldavas ümbrises, mis asub hoiukohas, mis vastab vastava tasemega salastatud teabekandjate hoiukohale seatud tingimustele, või Välisluureameti heakskiidetud krüpteerimismeetodiga krüpteerituna. Salasõnade hoidmise ja kasutamise protseduur on kirjeldatud süsteemi turbejuhendis. Salasõna kasutamine dokumenteeritakse.	Jah	Jah
15.	Süsteemi haldamiseks kasutab eriõigustega kasutaja eraldi isikustatud eriõigustega kasutajakontot.	Jah	Jah
16.	Internetiga või akrediteerimata sidevõrguga ühendatud süsteemile juurdepääsuks kasutatakse mitmikautentimist.	–	Jah
17.	Süsteem blokeerib kasutajakonto automaatselt pärast kolme edutut autentimiskatset vähemalt 15 minutiks.	Jah	Jah
18.	Süsteem teavitab kasutajat autentimise ebaõnnestumise põhjustest minimaalses võimalikus ulatuses.	Jah	Jah
Teabele juurdepääs			
19.	Süsteem võimaldab juurdepääsu vaid sellisele salastatud teabele, mille suhtes süsteemi kasutajal on põhjendatud teadmisvajadus ja juurdepääsuõigus. Töö- või teenistusülesandest tuleneva teadmisvajaduse muutumisel eemaldatakse eelnevast ülesandest tulenevad liigsed juurdepääsuõigused ning täiendatakse juurdepääsuõigusi vastavalt uuele ülesandele.	Jah	Jah
20.	Seansi alustamisel ilmub ekraanile teade süsteemi nime ning süsteemis töödeldava teabe kõrgeima salastatuse taseme kohta.	Jah	Jah
21.	Süsteem võimaldab kasutajal katkestada teabele juurdepääsu, sealhulgas lukustada ekraani.	Jah	Jah
22.	Kui süsteemi ei kasutata 15 minutit või rohkem, katkeb juurdepääs teabele ning rakendub seansi lukustumine.	Jah	Jah
23.	Süsteemi kasutajakonto, mida ei ole kasutatud 180 päeva jooksul, desaktiveeritakse.	Jah	Jah

24.	Süsteemi salastatud teavet töötlevale füüsilisele osale paigaldatakse selle volitamata avamise tuvastamist võimaldav unikaalse numbriga turvavahend. Turvavahendite üle peetakse arvestust ja tehakse regulaarseid kontrolle nende andmete õigsuse üle.	Jah	Ei
25.	Süsteemi salastatud teavet töötlevale füüsilisele osale paigaldatakse selgelt loetav märgistus süsteemis töödeldava teabe kõrgeima salastatuse taseme kohta.	Jah	Jah
26.	Süsteemi kaabeldus on ühenduskohtades visuaalselt eristatav ja tuvastatav ning kirjeldatud süsteemi turbejuhendis.	Jah	Jah
Logimine			
27.	Süsteem salvestab süsteemi kasutamise analüüsiks vajaliku info (sealhulgas käivitamine ja sulgemine, kasutaja sisenemine ja väljumine, muudatused kasutajate ja kasutajagruppide kasutajaõigustes, muudatused logiinformatsiooni seadistustes, kellaaja ja kuupäeva muutmine ja ebaõnnestunud katsed süsteemi siseneda, teabe üleviimine välisele teabekandjale).	Jah	Jah
28.	Süsteem salvestab salastatud teabe töötlemiseks kasutatava rakendusteenuse kasutamise analüüsiks vajaliku info (sealhulgas rakendusteenuse käivitamine ja sulgemine, kasutaja sisenemine ja väljumine, rakendusteenuse tõrked, suuremahulised konfiguratsioonimuudatused, info teabe edastamise kohta, muudatused kasutajate ja kasutajagruppide kasutajaõigustes, rakendusteenuses eriõiguste kasutamine ning muutmine).	Jah	Jah
29.	Süsteemis ja rakendusteenuses logitakse igakordne salastatud teabe töötlemine eesmärgiga tagada teabe töötlemise jälgitavus.	Jah	Jah
30.	Logiinformatsiooni kirje sisaldab sündmuse toimumise kuupäeva, kellaaega, liiki ja märget sündmuse õnnestumise või ebaõnnestumise kohta ning seob kasutajanime selle olemasolul logitava sündmusega.	Jah	Jah
31.	Eelnevates punktides nimetatud süsteemi logiinformatsioon säilitatakse.	Jah, vähemalt viis aastat	Jah, vähemalt kolm aastat
32.	Juurdepääs logiinformatsioonile on vastava õigusega kasutajal.	Jah	Jah
33.	Süsteem võimaldab logiinformatsioonist raportite ja väljavõtete tegemist inimloetaval kujul.	Jah	Jah

34.	Logiinformatsiooni säilitatakse viisil, mis tagab selle säilivuse jätkusuutlikkuse, võimaluse korral väljaspool süsteemi.	Jah	Jah
35.	Süsteemi logiinformatsiooni varundamise sagedus, varukoopiate säilitusnõuded ja juurdepääsuõigused varukoopiatele sätestatakse süsteemi turbejuhendis.	Jah	Jah
Pahavaratõrje			
36.	Viiruse või muu pahavara avastamiseks ette nähtud tarkvara on installeeritud kõigisse serveritesse ja tööjaamadesse ning konfigureeritud viisil, kus kontrollimine toimub automaatselt.	Jah	Jah
37.	Viiruse või muu pahavara avastamiseks ja tõrjeks ette nähtud tarkvara uuendatakse regulaarselt.	Jah	Jah
38.	Süsteemi sisenev teave kontrollitakse (võimaluse korral süsteemist eraldatud seadmega) viiruste või muu pahavara avastamiseks ja tõrjeks enne teabega tutvumist, sealhulgas enne faili avamist.	Jah	Jah
39.	Uus tarkvara kontrollitakse enne süsteemis kasutusele võtmist süsteemiväliselt viiruse või muu pahavara avastamiseks ja kõrvaldamiseks. Võimaluse korral võrreldakse tarkvara räsi väärtust originaali andmetega.	Jah	Jah
40.	Süsteemile tehakse regulaarselt viiruse või muu pahavara täiskontrolli.	Jah	Jah
41.	Süsteemis avastatud viirust või muud pahavara käsitletakse kui intsidenti.	Jah	Jah
42.	Viiruse või muu pahavara avastamiseks ette nähtud tarkvara kõiki teavitusi kontrollitakse regulaarselt.	Jah	Jah
Konfiguratsioonihaldus			
43.	Süsteemis kasutatava riistvara üle peetakse arvestust.	Jah	Jah
44.	Süsteemis kasutatava tarkvara üle peetakse arvestust.	Jah	Jah
45.	Süsteemis kasutatav tarkvara peab pärinema autentsest allikast.	Jah	Jah
46.	Süsteemis ei kasutata tootjast tuleneva suure riskiga riistvara, mis võib ohustada riigi julgeolekut.	Jah	Jah
47.	Süsteemis kasutatav tarkvara on ajakohane, turvauuenduste toega ning seda uuendatakse regulaarselt.	Jah	Jah
48.	Tootjapoolse toeta või teadaolevate turvanõrkustega riistvara, tarkvara, rakendused ja teenused, millest tulenevaid riske ei saa maandada, eemaldatakse kasutusest.	Jah	Jah

49.	Tarkvara seadistatakse võimaluse korral tugevdamise juhiste kohaselt.	Jah	Jah
50.	Süsteemi serverite ja tööjaamade riist- ja tarkvaraline konfiguratsioon dokumenteeritakse.	Jah	Jah
51.	Riist- ja tarkvara konfigureerib süsteemi eest vastutav eriõigustega kasutaja või väline teenuseosutaja süsteemi eest vastutava eriõigustega kasutaja järelevalve all.	Jah	Jah
52.	Riist- ja tarkvara konfigureeritakse minimaalse vajaliku funktsionaalsusega. Riist- ja tarkvara, mida süsteemis ei kasutata, eemaldatakse.	Jah	Jah
53.	Riist- ja tarkvara vaikimisi salasõnad muudetakse esmasel kasutuselevõtul. Süsteemis ei kasutata riist- ja tarkvara, mille salasõnu ei ole võimalik muuta.	Jah	Jah
54.	Serverite ja tööjaamade konfiguratsiooni vastavust dokumentatsioonile kontrollitakse regulaarselt. Kõigi sama tüüpi seadmete seadistamisel järgitakse samu aluskonfiguratsioone.	Jah	Jah
55.	Süsteemi kuupäeva ja kellaaja õigsust jälgitakse regulaarselt. Süsteemi kõigi osade jaoks kasutatakse sama ajaallikat.	Jah	Jah
56.	Süsteemis kasutatava riistvara ühendamine välisseadmetega, nende seadmete kasutamine või kasutamise tõkestamine kirjeldatakse süsteemi turbejuhendis.	Jah	Jah
	Terviklus		
57.	Süsteemis sisalduvast salastatud teabest säilitatakse ajakohane varukoopia.	Jah	Jah
58.	Süsteemis sisalduva salastatud teabe varundamise sagedus, varukoopiate säilitusnõuded ja -tähtajad ning juurdepääsuõigused varukoopiatele sätestatakse süsteemi turbejuhendis.	Jah	Jah
	Täiendav turbekorraldus		
59.	Süsteemi kasutajaid teavitatakse enne süsteemi kasutamist nende kohustustest süsteemi turvalisuse tagamisel.	Jah	Jah
60.	Kaamera ja mikrofoni kasutamisel lähtutakse minimaalsuse printsiibist ning nende kasutamine kooskõlastatakse Välisluureametiga.	Jah	Jah
61.	Süsteemi riistvara hooldatakse või parandatakse süsteemi sisemises turvakeskkonnas. Juhul, kui süsteemi riistvara on vaja hooldada või parandada väljaspool sisemist turvakeskkonda, tuleb kõik salastatud teavet sisaldada võivad komponendid riistvarast eemaldada ja jätta sisemisse turvakeskkonda.	Jah	Jah

62.	Süsteemi hooldamise ja parandamise tööd dokumenteeritakse viisil, millest nähtub, milliseid muudatusi ja millal on tehtud, kes muudatused tegi ning mis on muudatuste põhjus.	Jah	Jah
63.	Süsteemis tehakse pidevat seiret selle turvalisust ohustava tegevuse tuvastamiseks. Süsteemi logisid jälgitakse regulaarselt ning püütakse avastada kõrvalekaldeid tavapärasest tööst.	Jah	Jah
64.	Süsteemis toimunud intsidente hallatakse vastavalt süsteemi kasutusjuhendis sätestatud korrale ning nende menetlemine dokumenteeritakse.	Jah	Jah
65.	Õigus teisaldatavalt salvestuskandjalt salastatud teavet süsteemi salvestada on üksnes vastava õigusega kasutajal.	Jah	Jah
66.	Õigus teisaldatavale salvestuskandjale salastatud teavet salvestada on üksnes vastava õigusega kasutajal.	Jah	Jah
67.	Süsteemis ei kasutata otse tööjaamade vahel failide vahetamist võimaldavaid rakendusteenuseid.	Jah	Jah
68.	Süsteemi haldamiseks kasutatakse üksnes selleks mõeldud ja hallatavatest kohtvõrkudest eraldi olevat kohtvõrku.	Jah	Jah
69.	Süsteemis olevad erineva kasutusotstarbega osad on eraldi kohtvõrkudes.	Jah	Jah
70.	Süsteemi kõik kasutajad läbivad regulaarselt IT-turvalisuse ja -teadlikkuse koolituse, mis sisaldab vähemalt e-posti turvalisust (kaasa arvatud õngitsemine), interneti turvalisust, mobiilsete seadmete turvalisust, andmete kaitset, pahavara, manipuleerimisvõtteid ja organisatsiooni siseohte. Eriõigustega kasutajad läbivad lisaks süsteemi haldamisega seotud IT-turvalisuse koolituse vähemalt korra aastas.	Jah	Jah
71.	Süsteemi asukoht, seadmed ja paigaldus peavad vastama kiirgusturbe tagamise nõuetele.	Jah	–
72.	Salastatud teabe kaitseks kasutatakse nõuetele vastavaid ja Välisluureameti heakskiidetud krüptolahendusi.	Jah	Jah
Arvutivõrgud			
73.	Koht- või laivõrku ühendatud seadmete üle peetakse ajakohast võrguskeemi.	Jah	Jah
74.	Süsteemi sisemisest turvakeskkonnast väljuv salastatud teave krüpteeritakse nõuetele vastavate krüptomaterjalidega või seda	Jah	Jah

	kaitstakse volitamata juurdepääsu eest muu Välisluureameti lubatud meetodiga.		
75.	Süsteemi ühendamisel teise süsteemiga on tagatud salastatud teabe kontrollitud liikumine (näiteks ühesuunaline lüüs, tulemüür, sissetungi avastamise tarkvara) süsteemide vahel.	Jah	Jah
76.	Süsteemide ühendamisel ei tohi kõrgema tasemega salastatud teave liikuda madalama tasemega süsteemi. Eriliigilise salastatud teabe korral ei tohi teave liikuda süsteemi, kus seda teavet töödelda ei ole lubatud.	Jah	Jah
77.	Süsteemi perimeetri kaitse vahendite seadistused ning ühendused teiste süsteemidega dokumenteeritakse.	Jah	Jah
78.	Süsteemi perimeetri kaitse vahendid ei tohi asuda nende poolt kaitstavate virtuaalserveritega samas füüsilises serveris.	Jah	Jah
79.	Süsteemi perimeetri kaitse vahendid peavad paiknema töötleva üksuse sisemises turvakeskkonnas viisil, et neile on iseseisev juurdepääs vaid volitatud isikutel.	Jah	Jah
80.	Süsteemi perimeetri kaitse vahendite toimimist testitakse pärast nende paigaldamist ja seadistamist. Testi tulemused dokumenteeritakse.	Jah	Jah
81.	Süsteemi skaneeritakse vähemalt korra aastas selle haavatavuse tuvastamiseks.	Jah	Jah
82.	Süsteem on eraldatud internetist ja akrediteerimata sidevõrgust.	Jah	Ei
83.	Süsteemi ühendused sisse ja välja seadistatakse valge nimekirja põhimõttel.	–	Jah
84.	Jaostunneldust ei kasutata.	Jah	Jah
85.	Süsteemis kasutatakse turvalise e-posti lüüsi, mis pakub pahavara ja rämpsposti kaitset süsteemi perimeetril.	Ei	Jah
Süsteemispetsiifilised nõuded			
Kaasaskantavale töötlusseadmele rakendatavad lisanõuded			
86.	Kaasaskantavate töötlusseadmete ja nende kasutajate üle peetakse eraldi arvestust selliselt, et töötleval üksusel on igal ajahetkel teave, kelle käes seade on.	Jah	Jah
87.	Kaasaskantava töötlusseadmega võib avalikus ruumis teavet töödelda üksnes vastava õigusega kasutaja.	Jah	Jah
88.	Kaasaskantava töötlusseadme abil avalikus ruumis töödeldavat salastatud teavet ei säilitata töötlusseadmes oleval salvestuskandjal, välja arvatud juhul, kui see teave on krüpteeritud nõuetele vastavate krüptomaterjalidega või seda kaitstakse	Jah	Jah

	volitamata juurdepääsu eest muu Välisluureameti lubatud meetodiga.		
89.	Avalikus ruumis kaasaskantaval töötlusseadmel ei ole nähtavat märgistust, mis viitab salastatud teabe töötlemisele.	Jah	Jah
90.	Kaasaskantava töötlusseadme abil edastatava heli vahendusel salastatud teabe avalikus ruumis töötlemisel (rääkimisel ja kuulamisel) peavad edastaja ja vastuvõtja teavitama teist poolt oma viibimisest avalikus ruumis.	Jah	Jah
91.	Kaasaskantava töötlusseadme abil salastatud teabe avalikus ruumis töötleja peab seda tegema viisil, kus ta on enne veendunud, et juures ei viibi teisi juurdepääsuõiguse või teadmisvajaduseta isikuid.	Jah	Jah
92.	Kaasaskantava töötlusseadme puhul peavad seadme tööks mittevajalikud raadioliidesed, näiteks Wi-Fi, Bluetooth jm, olema välja lülitatud.	Jah	Jah
93.	Kaasaskantavat töötlusseadet peab töötlev üksus saama hallata.	Jah	Jah
94.	Kaasaskantavat töötlusseadet peab olema võimalik kasutuskõlbmatuks muuta.	Jah	Jah
Mobiilsidesüsteemidele rakendatavad lisanõuded			
95.	Mobiilsideseadme SIM-kaart peab olema kaitstud PIN-koodiga. PIN-kood ei tohi olla lihtsasti ära arvatav.	Jah	Jah
96.	Mobiilsideseadmele juurdepääsuks kasutatakse PIN-koodi, salasõna või Välisluureameti heakskiidetud muid meetodeid.	Jah	Jah
97.	Mobiilsideseadmele ligipääsu andev PIN-kood või salasõna ei tohi olla lihtsasti ära arvatav. PIN-koodil on miinimumpikkus.	Jah, 8-kohaline	Jah, 8-kohaline
98.	Mobiilsideseade peab ennast viima tehase algseadistusse pärast määratud kordi järjest valesti sisestatud PIN-koodi või salasõna.	Jah, viis korda	Jah, kümme korda
99.	Mobiilsideseadmed peavad olema kehtiva tootjapoolsete turvauuenduste toega, elutsükli lõpus olevad mobiilsideseadmed asendatakse aegsasti sobiva ning turvauuenduste toega lõppkasutaja seadmega.	Jah	Jah
100.	Mobiilsideseadme ühendused internetti või akrediteerimata sidevõrku lubatakse üksnes nn valge nimekirja alusel. Lubatud ühenduste kohta peetakse arvestust ning nimekiri vaadatakse vähemalt kord aastas üle.	-	Jah
101.	Mobiilsideseadmesse on lubatud paigaldada rakendusi üksnes nn valge nimekirja alusel. Lubatud rakenduste kohta peetakse arvestust ning nimekiri vaadatakse vähemalt kord aastas üle.	Jah	Jah

102.	Mobiilsideseadmes kasutatakse viiruse või muu pahavara avastamiseks ette nähtud tarkvara ja seda uuendatakse regulaarselt.	Jah	Jah
103.	Kui mobiilsideseadet ei kasutata, lukustub ekraan automaatselt.	Jah, 30 sekundi möödudes	Jah, 30 sekundi möödudes
Raadioseadmetele rakendatavad lisanõuded			
104.	Kui raadioseade ei ole volitatud kasutaja otseses valduses, peab seda hoiustama sisemises turvakeskkonnas.	Jah	Jah
105.	Raadioseade peab töötama määratud raadiosagedusel.	Jah	Jah
106.	Raadiosagedused tuleb planeerida nii, et ei esineks interferentsist tulenevaid raadiohäireid.	Jah	Jah
107.	Raadiosidesüsteemide topoloogia peab olema dokumenteeritud.	Jah	Jah
108.	Raadioseadmete konfiguratsioon peab olema dokumenteeritud.	Jah	Jah
109.	Raadioseadmetes peab kasutama Välisluureameti heakskiidetud krüptolahendusi.	Jah	Jah
110.	Raadiosidesüsteemide baasjaamad tuleb paigutada sisemisse turvakeskkonda nii, et neile on juurdepääs vaid volitatud isikutel.	Jah	Jah
Kõnesidesüsteemidele rakendatavad lisanõuded			
111.	IP-telefonid ja VOIP-serverid eraldatakse füüsiliselt või virtuaalselt (VLAN) teistest sama süsteemi osaks olevatest andmesideseadmetest.	Jah	Jah
112.	Kasutatakse krüpteerivaid signaliseerimis- ja meediatranspordi protokolle (TLS, SRTP) otspunktide vahel.	Jah	Jah
113.	Traadita ühendus, sealhulgas ühendus kõnetoru või peakomplektiga, on keelatud. Kõnesideseadmed, välja arvatud mobiilsideseadmed, ei tohi sisaldada raadioliideseid, näiteks Wi-Fi, Bluetooth.	Jah	Jah
114.	Erineva salastatuse tasemega kõnesidet võimaldav süsteem peab kõne alguses ja vajaduse korral selle kestel andma pooltele audio- või visuaalse teatega märku süsteemide vahel töödelda lubatud teabe kõrgeima salastatuse taseme kohta.	Jah	Jah
115.	Kõnesideseadmete juurdepääs sidevõrgule on kontrollitav.	Jah	Jah
116.	Tarkvaratelefoni (*softphone*) peakomplekt/kõnetoru on füüsiliselt välja lülitatav või arvutist eraldatav.	Jah	Jah
117.	Kõnesideseadme automaatne kõne vastuvõtmine on keelatud, välja arvatud automaatvastaja abil.	Jah	Jah

118.	Juurdepääs automaatvastaja funktsioonile on kaitstud salasõna või PIN-koodiga.	Jah	Jah
119.	Kõnesideseadme funktsioonidele kaugjuurdepääs (näiteks automaatvastaja juhtimine) teiselt tavaabonendilt on keelatud. Eriõigusega abonendi konfigureerimise funktsioon on kaitstud salasõna või PIN-koodiga.	Jah	Jah
120.	Kõnesidesüsteemil peab olema aktiveeritud kõnede logimine.	Jah	Jah
Salastatud välisteavet sisaldava töötlussüsteemi lisanõuded			
121.	Salastatud välisteavet sisaldava töötlussüsteemi puhul kohaldatakse välislepingust tulenevaid või rahvusvahelise organisatsiooni kehtestatud teabe kaitse nõudeid.	Jah	Jah

Kui tabelis on märgitud „Jah”, siis tuleb nõuet kohaldada.
Kui tabelis on märgitud „Ei”, siis ei pea nõuet kohaldama.
Kui tabelis on märgitud „–”, siis ei saa nõuet kohaldada.