

MFN 2020-11

Üldnõuded
Dokument ja selle lisad määratlevad mittefunktsionaalsed nõuded Keskkonnaministeeriumi (KeM) ja tema haldusala asutuste uutele infosüsteemidele
Nõuded on kohustuslikud ka olemasolevate infosüsteemide lisaarendustele ja versiooniuuendustele mahus, mis on lisaarenduse ja
Kui mõnda nõuet ei ole pakkuja arvates võimalik või otstarbekas täita, tuleb selle mittetäitmise fakt ja põhjendus pakkumuses välja tuua.
Nõuded on kohustuslikuks täitmiseks kõikidele tulemitele.
Alternatiivsete, käesolevas mittefunktsionaalsete nõuete dokumendis puuduvate tehnoloogiate, vahendite ja meetodikate valikul rakendab hankija
Kui mõnda konkreetselt kohalduvat nõuet ei ole pakkuja arvates võimalik või otstarbekas täita, tuleb selle mittetäitmise fakt ja põhjendus pakkumuses
Kõik erikokulepped fikseeritakse tellijaga kirjalikku taasesitamist võimaldaval viisil.

Nr	Nõude kirjeldus	Märkus
	Vastavus standarditele ja seadusandlusele	
1	Lahendus peab vastama dokumendis „Riigi infosüsteemi koosvõime raamistik“ kirjeldatud põhimõtetele.	Raamistik on leitav: https://www.mkm.ee/sites/default/files/riigi_it_koosvoime_raamistik.pdf
2	Lahendus peab vastama dokumendis "Infoturbe koosvõime raamistik" kirjeldatud põhimõtetele.	Raamistik on leitav: https://www.mkm.ee/sites/default/files/infoturbe_raamistik.pdf
3	Lahendus peab vastama dokumendis „Veebide koosvõime raamistik“ kirjeldatud põhimõtetele.	Raamistik on leitav: https://www.mkm.ee/sites/default/files/veebide_raamistik.pdf
4	Lahendus peab vastama „Eesti avaliku teabe masinloetava avalikustamise roheline raamat“ sõnastatud põhimõtetele ja nõuetele.	Dokument on leitav: https://www.mkm.ee/sites/default/files/avaliku-teabe-masinloetava-avalikustamise-roheline-raamat-20141125_0.odt
5	Lahendus peab vastama „Aadressiandmete süsteem“ määruses kehtestatud aadressiandmete nõuetele	Määrus on leitav https://www.riigiteataja.ee/akt/113102015002
6	Lahenduses tuleb tegevusalade määramiseks kasutada Eesti Majanduse Tegevusalade Klassifikaatorit (EMTAK).	Klassifikaator on leitav: https://emtak.rk.ee/EMTAK/pages/klassifikaatorOtsing.jsp
7	Lahendus peab vastama „Avaliku teabe seaduses“ kehtestatud teabe avalikustamise ja juurdepääsu võimaldamise nõuetele.	Seadus on leitav: https://www.riigiteataja.ee/akt/114032011019?leiaKehtiv

8	Lahendus peab vastama „Riigi infosüsteemi haldussüsteem“ (edaspidi RIHA) esitatud nõuetele ja reeglitele.	Määrus on leitav: https://www.riigiteataja.ee/akt/12933746?leiaKehtiv
9	Lahendus peab vastama „Infosüsteemide turvameetmete süsteem“ esitatud nõuete alusel määratud turbeastmele M, kui ei ole nõutud teisiti.	https://www.riigiteataja.ee/akt/13125331?leiaKehtiv Täpne rakendamise ulatus lepitakse kokku lähtuvalt konkreetsest infosüsteemist. Täpne rakendamise ulatus lepitakse kokku lähtuvalt konkreetsest infosüsteemist. ISKEga seotud materjal on leitav: https://iske.ria.ee/8_03/
10	Loodav lahendus peab vastama isikuandmete kaitse üldmäärusele ja direktiivile andmete edastamisel politseikoostöö ja õiguslase koostöö valdkonnas sätetele.	
11	Lahenduses peavad X-tee teenused olema realiseeritud vastavalt RIA poolt kirjeldatud nõuetele.	Nõuded on leitavad: https://www.ria.ee/ee/xtee-juhendid.html
12	Lahendus peab vastama "Infosüsteemide andmevahetuskiht" määruses kirjeldatud põhimõtetele.	Määrus on leitav: https://www.riigiteataja.ee/akt/127092016004
13	ID-kaardi allkirjastamislahenduse kasutamisel eelistatakse SiGa veebiteenuse kasutamist.	
14	Kuupäeva ja aja (kuupäev, kellaeg, ajaintervall) talletamisel teksti kujul tuleb aluseks võtta ISO 8601 standardis kirjeldatud põhimõtted.	Põhimõtted on leitavad: https://en.wikipedia.org/wiki/ISO_8601 või http://www.w3.org/TR/NOTE-datetime
15	Veebirakenduse kasutajaliides peab vastama vähemalt WCAG 2.1 tasemele AA.	Soovituste kogum on leitav: http://www.w3.org/TR/WCAG21
16	Veebipõhine kasutajaliides peab ühilduma HTML ja CSS standarditega.	Standardiseerimata HTML ja CSS kasutamine peab olema eelnevalt tellijaga kooskõlastatud.
Arhitektuur		
17	Realiseeritud lahendus peab tellija poolt kinnitatud arhitektuurile vastavalt töötama tellija poolt nõutud funktsionaalsete ja mittefunktsionaalsete nõuete ulatuses.	
18	Kõik infosüsteemis kasutatavad komponendid peavad olema tuvastatavad, põhjendatud ja dokumenteeritud.	
19	Kõik lahenduses kasutatavad kolmanda osapoole komponendid (nt välised süsteemid, teegid) peavad olema tuvastatavad ja dokumenteeritud.	
20	Liidesed väliste süsteemidega peavad olema standardsed (allutatud samastele reeglitele) ja liidestamise detailid peavad olema dokumenteeritud.	

21	Rakenduse liidesed peavad olema tõrkekindlad.	Lõppkasutaja peab saama jätkata rakenduse kasutamist ulatuses, mis on protsessiliselt võimalik. Süsteem peab tõrke korral võimalikult lühikese aja jooksul väljastama asjakohase veateate.
22	Infosüsteemide platvormid (nt rakendusserver, andmebaas) ja topoloogia peavad olema tellijaga kooskõlastatud enne reaalse tarkvaraarenduse algust.	Detailne infrastruktuur on kirjeldatud KeM haldusala tehnoloogilises profiilis.
23	Kõik arendamisel kasutatud komponendid peavad vastuvõtmise hetkel olema viimased stabiilsed versioonid.	
24	Infosüsteemi ülesehituses peab kasutama kolmekihilist arhitektuuri: andmekiht, kontrolleri kiht (äri loogika) ja esitluskiht.	
25	Infosüsteem peab olema üles ehitatud nii, et eessüsteemid (inglise k front end) ja tagasüsteemid (inglise k back end) on arhitektuuriliselt selgelt lahutatud.	
26	Andmebaasid ja rakendused peavad kasutama UTF-8 kodeeringut.	
27	Andmebaasi objektide nimed peavad olema sisulised ja andma aimu nende otstarbest.	
28	Lahendused peavad olema projekteeritud laiendatavana ja edasi arendatavana.	
29	Komponendid peavad olema sõltumatud ja taaskasutatavad.	Tuleb kasutada KEMITi olemasolevaid komponente (nt AUP, GEOSERVER jne.). Detailne infrastruktuur ja komponendid on kirjeldatud: KeM haldusala tehnoloogilises profiilis. Erandjuhud tuleb kooskõlastada tellijaga.
30	Rakendust peab saama liigutada ilma ümberprogrammeerimiseta erinevate domeenide, domeenisaitide ja keskkondade vahel.	
31	Rakendusel peab olema haldusliides.	Haldustoimingute tegemine otse andmebaasis peab olema viidud miinimumini. Peakasutajal peab olema selge ülevaade kasutajate õigustest.
32	Kui rakendused saadavad e-kirju, siis peavad nad selleks kasutama välist e-posti serverit.	
33	Rakendus peab suutma kasutada keskkonnamuutujaid.	
34	Arhitektuur peab olema modulaarne, teenustepõhine.	
35	Ebaõnnestunud logimiste arvu peab saama piirata ajaühiku kohta.	Muudatusi (logimiste arv, ajaühik) peab saama seadistada konfiguratsioonifailis.
36	Klientrakendus ei tohi teostada otsepöördust andmebaasi poole.	Võib kasutada rakendusserverit või adapterit.
37	Rakenduse failid, mis ei tohi olla kasutajale nähtavad, peavad olema kaitstud (rakenduse kasutajale mittekättesaadavates) kaustades.	
38	Sorteerimisreeglistik peab vastama eesti tähestikule, tõstutundlikkus peab olema väljalülitatud.	

39	Lihtsamatele päringutele (nt ühe konkreetse andmeobjekti otsing) peab loodav lahendus vastama maksimaalselt 2 sekundi jooksul.	
40	Keerulisemate päringute (nt nimekirja filtreerimine) puhul on ajaline piirang 5 sekundit.	
41	Loodav lahendus peab võimaldama serveri poolt lõppkasutajale tagastatavate andmeobjektide arvu piirangut ja/või mahukate andmekomplektide lehekülgaotust (inglise k pagination või lazy load).	
42	VM'i paigaldatava akenduse arendamisel tuleb arvestada, et KEMITis on vaikimisi kasutusel järgmised turbemoodulid: ModSecurity, SELinux.	
43	Kui rakenduse toimimiseks on vajalik autentimine, tuleb selleks kasutada KEMITi autentimislahendust AUP või RIA TARA.	
44	TARA või AUP ees on soovituslik kasutada Keycloak tarkvara.	
	Turvalisus, sh infoturve	
45	Välisele kasutajatele mõeldud rakendustes ei ole kasutajanime ja parooliga autentimine lubatud.	
46	Rakenduse autentimise jõustamine peab toimuma serveri poolel.	
47	Ebaõnnestunud autentimine peab lõppema viisil, mis ei jäta ründajale võimalust rakendusse sisse tungida ega tohi võimaldada kasutajale ligipääsu süsteemi toimimise informatsioonile.	Täpsem kirjeldus on leitav ISKE meede M4.400 "Turbe seisukohalt oluliste andmete väljastamine veebirakendustes". Meede on leitav: https://iske.ria.ee/8_03/ISKE_kataloogid/7_Kataloog_M/M4/M_4.400
48	Rakendus (sh konteineris käitav) ei tohi töötamiseks vajada root/administraatori õigusi.	
49	Autentimist võimaldav informatsioon (nt autentimissaladused, API võtmed, salasõnad) ei tohi sisalduda lähtekoodis ega võrgus olevates lähtekoodi repositooriumites.	
50	Rakenduse kasutajale kuvatavad URL-id ei tohi sisaldada isikuandmeid.	
51	Rakendusel peab olema konfigureeritav kasutajaseansi aegumise aeg.	
52	Süsteemist väljumine peab toimuma kasutajale üheselt arusaadaval ja turvalisel viisil. Seansist väljumine toimub kahel viisil: kasutaja seansi lõpetab süsteem, sest seanss on olnud pikem kui süsteemile seadistatud vaikimisi limiit või kasutaja lõpetab seansi omal soovil.	
53	Süsteem peab teavitama kasutajat sessiooni lõppemisest.	
54	Kasutajal peab olema igal süsteemi kasutamise ajahetkel võimalik seanss omal soovil lõpetada.	
55	Iga eduka süsteemi sisselogimise (autentimise) korral tuleb alati luua unikaalne seansi identifikaator (inglise k session ID)	

56	Seansi identifikaator ei tohi kajastuda ressursilokaatoris (URL-is), veateadetes ega logides.	
57	Seansi identifikaator peab olema piisava pikkusega, juhuslik ja unikaalne kogu aktiivse seansi jooksul.	
58	Rakendus ja selle komponendid peavad võimaldama keskkondade lahusust (nt arendus-, test- ja toodangu keskkond).	
59	Andmebaasis olevate rakenduste kontod peavad omama ainult minimaalselt rakenduse tööks vajalikke õigusi.	
60	Krüptoalgoritmide ja räsifunktsioonide kasutamisel tuleb järgida RIA veebilehel avaldatud krüptograafiliste algoritmide elutsükli uuringu värskemal versioonis toodud soovitusi ja põhimõtteid.	Uuring on leitav: https://www.ria.ee/ee/kruptouuringud.html
61	Rakenduses peab olema tagatud võimekus välja vahetada aegunud ja ebaturvalisi krüptoalgoritme.	Krüptoalgoritmide väljavahetamine peab olema dokumentatsioonis kirjeldatud.
62	Kõik paroolid ja salasõnad peab rakendus salvestama kas räsituna ja soolatuna või krüpteeritud kujul.	Krüpteerimise kasutamisel peab protseduur olema kirjeldatud ISKE meetmes M 4.401 „Konfidentsiaalsete andmete kaitse veebirakenduses“ toodud nõuetest lähtuvalt.
63	Kõik võtmed ja salasõnad peavad olema asendatavad ning need tuleb toodangu keskkonna installatsiooni ajal luua või asendada.	
64	Võrguliikluse krüpteerimiseks peab olema HTTPS valmidus.	
65	Tarkvara iga versioon peab läbima koodikvaliteedikontrolli süsteemi SonarQube nii, et pole Security, Blocker ja Critical tüüpi vigu.	
66	Rakendusse ja andmetele tohib olla ligipääs ainult dokumenteeritud ning kirjeldatud teid mööda ja dokumenteeritud autentimisprotseduure kasutades.	
67	Kui rakendus kasutab brauseri küpsiseid (inglise k session cookie) või muid tehnoloogiaid (nt local storage jm), mis salvestavad kasutaja arvutisse informatsiooni, siis tuleb kasutajat sellest eelnevalt teavitada.	
68	Rakendus ei tohi teostada X-tee päringut otse kasutaja arvutist.	
69	Rakendusserver ja andmebaas peavad olema võimelised töötama eraldi serveritel.	
70	Veebirakenduse kõik viited failidele ja kataloogidele peavad olema ilma absoluutse failiteeta.	
71	Kui rakenduse poolt töödeldavate andmete ISKE konfidentsiaalsuse klass on 2 või kõrgem, peab rakenduse andmemudel võimaldama lihtsate vahenditega andmete anonümiseerimist.	
72	Väliste kasutajatele mõeldud veebilehega rakendused peavad olema kaitstud keelatud päringute eest.	

73	Kui rakendus võimaldab mitteautenditud kasutajal edastada andmeid, tuleb need andmed puhastada XSS filtriga.	
74	Kui on nõutud andmete jälgimise rakendamine tuleb selleks kasutada RIA poolt pakutavat andmejälgijat.	https://github.com/e-gov/AJ/
75	Loodava lahenduse realiseerimiseks võib kasutada riigipilve tehnoloogiaid, järgima peab	Dokument „Nõuded riigipilvele“ on leitav:
76	RIA poolt koostatud dokumenti „Nõuded riigipilvele“.	https://www.ria.ee/riigiarhitektuur/wiki/lib/exe/fetch.php?media=an:riigipilve_alusnouded.pdf Informatsioon riigipilve kohta on leitav: http://riigipilv.ee/
Lähtekood		
77	Rakenduse kõikide versioonide täielikku lähtekoodi hoitakse KEMITi repositooriumis ja kood paigaldatakse sinna enne versiooni toodangusse minekut.	
78	Repositooriumi failide vaikimisi kodeering on UTF-8 ilma BOM signatuurita.	Välja arvatud juhtudel, kui tehnilises kirjelduses on tehnoloogiliste eripärade või muude piirangute tõttu sätestatud teisiti.
79	Repositooriumisse üleslaaditud lähtekood peab olema kompileeritav ilma muudatusteta.	
80	Repositooriumisse üleslaaditud lähtekood peab olema täielik ehk sellest saab koostada ja paigaldada täisfunktsionaalse rakenduse.	
81	Repositooriumisse tuleb korraga laadida kõik iga muudatusega seotud materjalid.	Enne materjalide üleslaadimist tuleb repositooriumust võtta viimane uuendatud koodi seis.
82	Materjalide üleslaadimisega peab kaasnema sisuline üleslaetavat materjali kirjeldav kommentaar.	
83	Rakenduse lähtekood peab olema kommenteeritud detailsusega, mis võimaldab erialast ettevalmistust omaval tarkvaraarendajal teostada süsteemi edasiarendust.	
84	Rakenduse lähtekood, kommentaarid, muutujate, tüüpide ja funktsioonide nimed peavad olema inglise keeles, sisulised ja andma aimu nende otstarbest.	
85	Koodis kasutatavad konstandid ja lühendid tuleb kirjutada suurtähtedega.	
86	Rakenduse lähtekood ei tohi sisaldada pöördumispunktide aadresse, paroole ega võtmeid (ka siis kui need on koodist väljakommenteeritud).	
87	Rakenduse lähtekoodis peab olema võimalik tuvastada muudatuse teinud konkreetne füüsiline isik.	
88	Lähtekood peab olema kompileeritav tellija poolt määratletud arenduskomplekti ja versioonidega.	Tellijal poolt aktsepteeritud Java kompilaatorid on ANT ja MAVEN. Alternatiivsete vahendite kasutamine on lubatud kui nende rakendamine on põhjendatud ja kooskõlastatud tellijaga.
89	Kasutuses mitteolev kood tuleb rakendusest eemaldada või selgelt eraldada.	

	Andmebaas	
90	Andmebaasi tabelid ja väljad peavad olema kommenteeritud. Kommentaarid peavad olema inglise keeles ja sisulised.	
91	Andmebaasi väljapikkused peavad olema väljendatud sümbolites (tähemärkide arv).	
92	Andmebaasi objektide nimetused peavad olema inglise keeles ning andma selget aimu otstarbest (va ajutised rakenduse poolt genereeritavad tabelid nn temp).	
93	Andmebaasi tabelite nimetused tohivad sisaldada ladina tähestiku väiketähti „a-z“, numbreid „0-9“, alakriipsu " ". Andmebaasi objekti nimetus ei tohi alata numbriga.	
94	Igas andmebaasi tabelis peab olema defineeritud primaarvõti (inglise k Primary Key).	
95	Andmebaasi objektide loomiseks tuleb kasutada tehnoloogilises profiilis toodud andmebaasi migratsioonivahendeid.	
96	Igas schema-põhises kataloogis peab olema ühine andmebaasi muudatuste paigaldamise skript, mis järjest käivitab vajalikke käske õiges järjekorras.	
97	Ühest andmetabelist teise viitamisel tuleb kasutada võõrvõtit (inglise k Foreign Key). Võõrvõtme nimi peab seostuma tabeli ja väljaga, millele see viitab.	
98	Kõik võõrvõtmed peavad olema indekseeritud.	
99	Kui rakenduse versioon nõuab andmebaasi muudatusi, peavad üleantava koodiga kaasas olema andmebaasi paigalduse migratsiooniskriptid.	
	Logimine ja monitooring	
100	Süsteemi muudatused ja rakenduse ning kasutajate tegevused logitakse seostatuna muudatuse/tegevuse teostanud konkreetse füüsilise isiku ja tema rolliga.	
101	Logiteadete sisu peab olema kirjutatud inglise keeles.	
102	Logimine peab olema konfigureeritav ning kasutada tuleb standardseid logiformaate, et võimaldada hilisem logianalüsaatorite kasutamine.	
103	Andmebaasi logidest saadetakse reaalajas koopia failisüsteemi logisse, mis peab sisaldama ka logimisfunktsionaalsuse aktiveerimise ja deaktiveerimise infot (nt aeg, kasutaja jm).	
104	Failisüsteemi logimisel peavad logid olema katalogiseeritud, üldlevinud faililaiendiga (nt .log, .txt, .xml) ja roteeruvad.	
105	Rakendus ei tohi väljastada kasutajale veateateid või aktiivsujälgi, mis sisaldavad seansi identifikaatorit või isikuandmeid.	
106	Sisselogimise mehhanismid peavad olema võimelised logima nii õnnestunud, kui ka ebaõnnestunud sisselogimise katseid.	
107	Rakendus peab omama sisemist meetrikat ja infot sündmuste kohta ning jagama seda vastavalt prometheus standardile.	Rakenduse peab jagama meetrikat aadressil /health
108	Rakenduse ärilogi(auditlog) andmebaas peab olema sõltumatu rakenduse tööbaasist.	

109	Kõik logid peavad olema kaitstud rakenduse kasutaja poolse lubamatu ligipääsu ja muutmise eest.	
110	Kui rakenduse ISKE konfidentsiaalsuse turvaosaklass on 2 või kõrgem (S2, S3) ja/või tervikluse turvaosaklass on 2 või kõrgem (T2, T3), peab rakendus logima andmete loomist, muutmist (sh kustutamist) ja vaatamist.	Turvaosaklasside S3 ja T3 korral peab rakendus logima ka administraatorite ja haldurite poolt tehtavaid andmete muudatusi (sh otse andmebaasis) ja vaatamisi.
111	Logimise tasandid on: DEBUG – arendamise etapis süsteemi olekut kirjeldav informatsioon (kasutatakse ainult arenduskeskkonnas) INFO – kasutaja päringute informatsioon, kasutaja infoteated (nt „Andmed salvestatud“, „Andmed muudetud“) WARNING – kasutajale kuvatav valest sisendist tekkiv oodatud viga (nt „Vigaselt sisestatud andmed“) ERROR – süsteemi vead, mis tekivad kasutaja sisendist (nt vigase andmebaasipäringu tekkimine) FATAL – rakenduse toimimise kriitilised vead, mis takistavad rakenduse tavapärasest toimimist (nt vigane konfiguratsioon)	
	Konfiguratsioon	
112	Kõik komponendid peavad olema ajakohase turvakonfiguratsiooniga ja versiooniga.	
113	Komponentide vaheline (nt rakendusserveri ja andmebaasi serveri) suhtlus peab olema krüpteeritud.	
114	Komponentide vahelise ühenduse jaoks tuleb kasutada minimaalselt vajalike õigustega kontot.	
115	Rakenduste omavahelisel suhtlemisel tuvastatakse üksteist OAuth2 abil.	
116	Rakendus peab olema aedikkäideldud, konteinerdatud või muul viisil isoleeritud, et takistada ründajal rakenduse kasutamist teise rakenduse ründamiseks.	
117	Rakenduse konfiguratsiooniparameetrid ei tohi muutmisel vajada uuesti kokku kompileerimist.	Eraldi konfiguratsioonifail võib olla kasutusel logimise ning arendaja ja administraatori vastutusala parameetrite jaoks.
118	Konfiguratsiooniparameetrite nimed peavad olema inglise keelsed ja sisulised.	Kui sisulist nime ei ole võimalik kasutada, siis peab kasutatava nime kõrval olema seletus.
119	Konfiguratsioonifailid peavad olema rakendusserveri tüübile vastavalt vaikimisi kaitstud.	
120	Samasisulisi konfiguratsiooni parameetreid ei tohi korduvalt kasutada, lubatud on kirjeldada ainult üks kord.	
	Kasutajaliides	
121	Kasutajaliidese kõik disainiotsused peavad olema tellijaga kooskõlastatud.	

122	Kasutajaliideste realiseerimiseks kasutatavad UI raamistikud ja komponendid tuleb tellijaga eelnevalt kooskõlastada.	
122	Ühe veebirakenduse realiseerimiseks kasutatavate erinevate UI raamistikute ja komponentide arv peab olema minimaalne.	
122	Kasutajaliidese kõik osad ja teated peavad olema eestikeelsed.	
122	Peale kasutaja sisselogimist rakendusse kuvatakse sisseloginud kasutaja nimi ja rolliinfo. Kui ühele kasutajatunnusele on määratud mitu rolli, kuvatakse kasutajale rollivalik.	
122	Kasutajaliides peab alati küsima kinnitust andmete kustutamise ja massmuutmise kohta.	
122	Kasutajal peab olema võimalik rakenduses tegevus pooleli jätta ja hiljem jätkata samast kohast ilma kohustuseta algusesse liikuda.	
122	Kasutajaliides peab veatult toimima brauseritega, mida toetab eID baastarkvara, kui hanke tehnilises kirjelduses ei ole nõutud teisiti.	eID poolt toetatav brauserite nimekiri on leitav: http://www.id.ee/?id=33993
122		Lahendus peab toetama brauserite versioone, mille kasutus on vähemalt 5% Eestis ning mille kasutustrend on kasvav.
122	Kõikide eelnevast nõudest välja jäävate brauserite kasutamise puhul peab kasutaja saama tõrke korral vastavasisulise teavituse.	Kasutajat tuleb teavitada mittetoetatud brauseri kasutamisest.
122	Veebilehitseja navigatsiooninupud peavad käituma rakenduses analoogiliselt klassikalise veebilehitsemisega (nt veebilehitseja „Tagasi“ nupp navigeerib kasutaja eelmisele kuvatud lehele).	
122	Kasutajaliideses navigeerumine peab lähtuma ärioloogikast ja võimaldama andmete sisestamist ning kasutamist ainult klaviatuuri kasutades.	
122	Kasutajaliidese toiminguni navigeerimiseks peab kehtima kolme klõpsu printsiip, väljalogimiseks ühe klõpsu printsiip.	
122	Interaktiivse vormi puhul ei tohi lehe värskendamise tegevust korrata (nt faili teistkordselt laadida, saadetud andmeid uuesti saata).	
122	Kui vorm koosneb mahukatest andmeväljadest, peab kasutajaliides eeldefineeritud ajavahemike järel salvestama välja sisu, et vältida sisestatud andmete kadumist.	Mahukad andmeväljad täpsustatakse/lepitakse kokku detailanalüüsi käigus arenduse teostamisel. Salvestamine puudutab vaid sisestamise vormi kohta.
122	Vormide puhul peab tellija poolt nimetatud väljal olles kuvama kasutajale juhised, mis kujul informatsiooni väljale sisestada tuleb.	
122	Andmete sisestamisel peab rakendus alati kontrollima, et sisestatud andmed vastavad välja tüübile.	
122	Rakendus peab võimalikult palju informatsiooni automaatselt eeltäitma (nt kirje sisestamise kuupäev).	

122	Kasutajaliides peab olema tõlgitav teise keelde ilma rakenduse lähtekoodi muutmata.	
122	Vältida tuleb kuvasid, mis eeldavad info lugemiseks kerimist paremale-vasakule.	
122	Kui rakenduses teostatav päring on pikem kui kolm sekundit, peab kasutajat sellest visuaalselt teavitama (nt ekraanil on liivakella kujutis; kuvatakse teade, et päringut teostatakse).	
122	Rakenduse esilehel peab olema võimalus halduri poolt lisada kasutajale mõeldud teavitusi ja informatsiooni.	
122	Kasutajaliides peab teavitama kasutajat ette seansi aegumisest.	
122	Veateade peab olema kirjutatud lühidalt, selges ja lõppkasutajale arusaadavas keeles. Süsteemi rikete tehnilisi üksikasju ei tohi välja näidata.	
122	Veateade peab sisaldama probleemi kirjeldust, vea koodi ja lahendust või infot, mis juhendab kasutajat edaspidiseks vea vältimiseks.	
122	Süsteem peab asendama vaikumisi veateate lehekülje, kuid säilitama algse HTTP vastuskoodi.	
Testimine		
123	Rakenduse kõik üleantavad versioonid peavad olema enne tellijale üleandmist täies mahus testitud: testitakse kõiki funktsionaalseid ja mittefunktsionaalseid nõudeid. Tellija nõudmisel tuleb arendajal koos rakenduse üleandmisega esitada testitulemuste raport.	
124	Rakenduse igakordsel versiooni üleandmisel tellijale, peab kaasas olema skript analüüsi käigus kokkulepitud jõudlustestide teostamiseks.	
125	Jõudlustestid peavad olema läbiviidud vähemalt kahekordse eeldatava koormuse varuga.	
126	Rakenduse koormuse testimiseks tuleb luua testandmete kogum.	
127	Loodav rakendus peab olema enne tellijale tarnimist testitud vimase kehtiva OWASP Top 10 väljatoodud turvanõrkuste vastu.	Testimistulemuste raport tuleb esitada tellijale rakenduse üleandmisel.
Dokumentatsioon		
128	Kogu rakenduse dokumentatsioon peab olema kirjeldatud korrektsetes eesti keeles.	Erandid võib olla kolmanda osapoole komponentide dokumentatsioon (dokumentatsioon, mis pole kirjutatud tellija jaoks). Erandina käsitletakse ka välise partneritega seotud projektdokumentatsiooni. Kõik erandid tuleb kirjalikku taasesitamist võimaldaval viisil kooskõlastada tellijaga enne dokumentatsiooni koostamist.
129	Dokumentatsioon peab olema eesti keeles ja sisaldama versiooni numbrit, muutmise kuupäeva, autori nime ja olema koostatud selge struktuuriga ja peab olema piisavalt selge, et Tellija iseseisvalt suudab selle järgi toimida.	Iga dokumendi versiooni kõik uuendused (võrrelduna eelmise kehtinud versiooniga), peavad olema visuaalselt eristatavad.

130	Lahenduse dokumentatsioon peab sisaldama RIHA määrusest tulenevat kohustuslikku informatsiooni.	RIHA määrus on leitav: https://www.riigiteataja.ee/akt/13147268?leiaKehtiv
131	Lahenduse dokumentatsioon peab sisaldama ISKE standardi meetmes M 2.574 „Tarkvaraarenduse põhjalik dokumentatsioon“ nõutud dokumente.	Meede on leitav: https://iske.ria.ee/8_02/ISKE_kataloogid/7_Kataloog_M/M2/M_2.574
132	Kõik dokumendis viidatud ja seotud teised dokumendid peavad olema tellijale edastatud enne dokumendi heakskiitmist tellija poolt.	
133	Kõik tellijale esitatud dokumendid peavad olema redigeeritavad enamlevinud redaktoritega (nt Microsoft Office, LibreOffice).	