Nõuded arendustele kehtiv versioon 7.0

Created by Taavi Meier, last updated on Feb 16, 2026 • 1 minute read

§Requirements

Key	Noude liik	Summary	Description	Status	T v
NA-1	Andmekvaliteet ja standardid	Loodavate lahenduste X-tee teenused peavad vastama RIA x-tee juhendis toodud nõuetele.		KEHTIV	A
NA-2	Andmekvaliteet ja standardid	Lahendusega koos tarnitav standardtarkvara peab vastama RIK nõuetele.	Kui hankes ei spetsifitseerita tarkvaralist lahendust tuleb kasutada vastaval konkreetsele vajadusel allpool toodud tarkvarade viimaseid stabiilseid versioone. Serverite operatsioonisüsteemina: 1) Linux RedHat Enterprise/Rocky 2) Windows Andmebaasidena: 1) Microsoft SQL 2) Postgre SQL 3) MariaDB Veebiserverina: 1) Nginx 2) Microsoft IIS 3) Apache Rakendusserverina: 1) Tomcat Programmeerimiskeelena : 1) C# 2) Java 3) Python Kui koos tarnega tarnitakse kommertstarkvara peab selle litsents sisaldama vähemalt 5 aasta turvaparandusi	KEHTIV	A
NA-3	Andmekvaliteet ja standardid	Rakendus peab olema loodud vastavalt Eesti Infoturbestandardi nõuetele.	Aluseks tuleb võtta hanke väljakuulutamise hetkel kehtiva versiooni meetmeid.	KEHTIV	A
NA-4	Andmekvaliteet ja standardid	Avalik sektor arendab riigi tarkvara eelkõige avatult ja avaldab tarkvara vaba litsentsiga vastavalt litsentsi nõuetele.	Antud nõudes võib erandeid teha ainult juhul, kui on teisiti ette nähtud seadusega või muul tellijaga kokku lepitud põhjendatud juhul. RIKis kasutatavad levinuimad vaba tarkvara litsentsid on EUPL, GNU GPL, MIT. Litsentsi valik sõltub vajadustest ja kohustustest ning tuleb kokku leppida tellijaga. Litsentside litsentsitingimustes sisalduvad nõuded, mida tuleb litsentsi kasutamisel täita, on järgmised: EUPLi puhul on nõutav mh: 1) autoriõiguse märge päises (Copyright © <aasta> <autori nimi>), mille järel on märge „Litsentsitud EUPL alusel“). GNU GPL puhul on nõutav mh: 1) autoriõiguse märge päises (Copyright © <aasta> <autori nimi>); 2) litsentsitingimustes ette nähtud teavitus töö osas garantii välistamise kohta.	KEHTIV	T

			MIT puhul on nõutav mh: 1) autoriõiguse märge päises (Copyright © <aasta> <autori nimi>) koos litsentsis ette nähtud teavitusega; 2) litsentsitingimustes ette nähtud teavitus töö osas garantii välistuse kohta. Täpsemalt tuleb nõuetega tutvuda lähtudes valitud litsentsitüübi litsentsitingimustest. Valitud litsentsi litsentsitingimused esitatakse ühel või mõlemal alljärgnevatest viisidest: 1) LICENCE-fail peab olema repositooriumis avalikustatud koos tarkvara koodiga; 2) litsentsitingimuste tekst iga faili päises; 3) lisades päisesse link asukohale, kus on võimalik litsentsitingimustega tutvuda.		
NA-5	Arhitektuur	Komponendid peavad olema sellised, mille eluea lõpp (EOL) pole teadaolevalt vähem kui 2 aasta pärast.	Erindid tuleb eraldi kokku leppida Strateegia tiimiga.	KEHTIV	A
NA-6	Arhitektuur	Infosüsteemide komponendid ja topoloogia peab olema enne reaalse arenduse algust RIK-iga kooskõlastatud.	Kooskõlastamist koordineerib Strateegia tiim (peaarhitekt).	KEHTIV	A
NA-7	Arhitektuur	Rakendusserver peab võimaldama töötamist andmebaasiserverist eraldi serveril.		KEHTIV	A
NA-8	Arhitektuur	Rakendust peab saama ilma ümber programmeerimata liigutada erinevate domeenide ja domeeni saitide vahel	Lahenduses ei tohi olla sisse kompileeritud absoluutseid URL-e.	KEHTIV	A
NA-9	Arhitektuur	Väliseid liidestusi peab olema nii vähe, kui võimalik.	Liideseid peab saama konfiguratsioonist välja lülitada. Väliste liidestuste veaolukorrad peavad olema käsitletud. Süsteem peab toimima mitte-ärikriitiliste liidestusteta.	KEHTIV	A
NA-10	Arhitektuur	Andmevahetus riigi infosüsteemi kuuluvate andmekogudega ja riigi infosüsteemi kuuluvate andmekogude vahel toimub läbi riigi infosüsteemi andmevahetuskihi (x-tee).	Avaliku teabe seaduse § 43 (9) lõige 5. Kui X-tee päringut teostab inimene, siis peab olema päringu päises autentinud kasutaja andmed.	KEHTIV	A
NA-11	Arhitektuur	Rakenduste keskkonnad peavad kasutama vastavate X-tee turvaserverite otspunkte.	Arendus vastu arenduse otspuntki jne.	KEHTIV	A
NA-12	Arhitektuur	Rakendus peab olema konfigureeritav ühest kohast ilma kompileerimisvajaduseta.	Konfiguratsiooni võib vajadusel automaatselt kopeerida, ilma muutmata, kesksest kohast mujale (näiteks helm chartis values failist kopeerimine mitmesse configmapi). Logimise seaded võivad olla rakenduse konfiguratsioonifailist eraldi ühes lisakonfiguratsioonifailis (näiteks Log4net).	KEHTIV	A
NA-13	Arhitektuur	Kompileeritud rakenduse paigaldamine peab toimuma mõistliku aja jooksul.	Mõistlik aeg on kuni 1 minut.	KEHTIV	A
NA-14	Arhitektuur	Rakendus peab olema 64-bitine.		KEHTIV	A

NA-15	Arhitektuur	Andmebaas ja rakendus peavad kasutama UTF-8 kodeeringut.	Nõue kehtib Oracle ja Postgre andmebaaside puhul. Erindid lepitakse eraldi Strateegia tiimiga kokku. Näiteks UTF-16.	KEHTIV	A
NA-16	Arhitektuur	Failid peab katalogiseerima aasta > kuu > kuupäev.	Täpsem lahendus leppida Strateegia tiimiga kokku.	KEHTIV	A
NA-17	Arhitektuur	Üldine programmeerimise paradigma on objekt-orienteeritud.	Erindid tuleb eraldi Strateegia tiimiga kokku leppida.	KEHTIV	A
NA-18	Arhitektuur	Kõik baasitabelite välisvõtmed peavad olema indekseeritud.	Indekseid ja muid meetmeid kasutatakse andmebaasi jõudluse tõstmiseks. Väliseid võtmeid tuleb kasutada ka ühest andmebaasist teisele viitamisel.	KEHTIV	A
NA-19	Arhitektuur	Tuleb kasutada päringumuutujaid (inglise keeles "Parameter Binding")	SQL päringute väljakutsumisel väljastpoolt andmebaasi peab kasutama päringumuutujaid, et vältida SQL vahemälu fragmenteerumist.	KEHTIV	A
NA-20	Arhitektuur	Andmebaasitabelites peab olema tehniline primaarvõti.	Nimetus peab olema „ID“	KEHTIV	A
NA-21	Arhitektuur	Failid ja failide indeks peavad olema replikeeritavad teise serveriruumi.	Failide hoidmise asukoht ja loogika on vastavalt kokkuleppele.	KEHTIV	A
NA-22	Arhitektuur	Haldustoimingute tegemiseks peab olema vastav haldusliides.	Eemärk on vähendada otse baasis tehtavaid toiminguid.	KEHTIV	A
NA-23	Arhitektuur	Andmebaas peab toetama külm- ja kuumvarundamist teise serveriruumi.	Ei tohi kasutada teenuseid, mis välistavad andmebaasi peegeldamist (nt "failstream").	KEHTIV	A
NA-24	Arhitektuur	Sorteerimisreeglistik peab vastama eesti keele tähestikule.	Peab kasutama case-insensitive, accent-sensitive sorteerimist.	KEHTIV	A
NA-25	Arhitektuur	Kasutama peab RIK-i elektronposti serverit.	Kirjade saatmine ja mall peavad olema konfigureeritavad. Juhul kui elektronposti server ei võta kirju vastu, siis tuleb need uuesti saata elektronposti teenuse taastumisel.	KEHTIV	A
NA-26	Arhitektuur	Konfiguratsiooniparameetrite nimed peavad olema sisulised.	Näiteks : X-tee Turvaserver, mitte XTTS või viitenumber, mitte vk_seb jne.	KEHTIV	A
NA-27	Arhitektuur	Ees- ja tagasüsteemid peavad olema arhitektuuriliselt selgelt lahutatud.	Ees- ja tagasüsteemid peavad olema eraldi paigaldatavad ja konfigureeritavad.	KEHTIV	A
NA-28	Arhitektuur	Konfiguratsioonifailid peavad olema vaikimisi kaitstud failid.	Näiteks IIS: *.config , *.resources Apache: *.conf, .htaccess. Kui neid on mitu, siis arendaja peab need eraldi välja tooma konfiguratsioonifailide listis.	KEHTIV	A
NA-29	Arhitektuur	Lõpp-kasutaja näeb vaid faile, mida ta peab nägema.		KEHTIV	A

NA-30	Arhitektuur	Konfiguratsioonis ei tohi olla sisult dubleerivaid parameetreid.	Kõiki parameetreid tuleks konfiguratsioonis kirjeldada vaid üks kord. Näiteks nii ei tohi olla: **connectionString** = "Server=myServerAddress;Database=myDataBase;User Id=myUsername;Password=myPassword;" **_cString** = "Server=myServerAddress;Database=myDataBase;User Id=myUsername;Password=myPassword;"	KEHTIV	A
NA-31	Arhitektuur	Rakendused peavad olema kõrgkäideldavad.	Meie arendatud rakendused ja kasutatavad karbitooted peavad olema kõrgkäideldavad. *Sticky sessionid* ei ole soovitatud, vajadus eraldi läbi rääkida.	KEHTIV	A
NA-32	Arhitektuur	Süsteemiintegratsioonid peavad klientrakendusele olema peidetud.	Näiteks klientrakendus ei tohi pöörduda otse andmebaasi ja x-tee poole.	KEHTIV	A
NA-33	Arhitektuur	Keskkonnapõhiseid muutujad peavad olema konfiguratsioonist seadistatavad.	Näiteks WSDL ei tohi sisaldada viiteid arendusserveritele.	KEHTIV	A
NA-34	Arhitektuur	Windows teenuste nimed peavad olema konfigureeritavad.		KEHTIV	A
NA-35	Arhitektuur	Andmebaasi ei tohi realiseerida rakenduse äriloogikat.	Andmebaas võib sissetulevate andmetega teha ainult tehnilisi tegevusi. Välja arvatud taustatööd. Näiteks õiguste arvutamine või unikaalsete võtmete genereerimine.	KEHTIV	A
NA-36	Arhitektuur	Andmebaasi peab olema võimalik viia MS-SQL standarditele.	Ei tohi kasutada platvormispetsiifilist lahendusi. Erindid eraldi kokku leppida Strateegia tiimiga.	KEHTIV	A
NA-37	Arhitektuur	Rakendus peab kasutama autentimiseks RIK poolt heaks kiidetud OpenID põhist autentimislahendust.	Autentimisviisid peavad olema konfigureeritavad. Samuti peab rakenduse konfiguratsioonist olema määratav, kas ID-kaardiga autentimise korral kasutatakse OCSP või tühistusnimekirjade põhist autentimist.	KEHTIV	A
NA-38	Arhitektuur	Uniform resource identifier (URI) pikkus ei tohi ületada ühegi IS poolt toetatava brauseri maksimaalset lubatud väärtust.	Max URI < 2000.	KEHTIV	A
NA-39	Arhitektuur	Rakenduse teenusekirjeldus peab olema üles ehitatud nii, et see toetaks teenuse versioneerimist.	Teenuste kirjelduses võimalike complexType versioonide väärtus "any"	KEHTIV	A
NA-40	Arhitektuur	Rakenduse operatiivbaas peab olema arhiveeritav.	Enamasti tehakse seda osadena, näiteks juriidiliselt aegunud menetlused, mida kasutajad enam ei näe.	KEHTIV	A
NA-41	Arhitektuur	Rakendusega tarnitavad litsentsid peavad olema vähemalt 5-aastase kehtivusajaga.	EU projektide korral tuleb kehtivusaja suhtes lähtuda EU või RIA nõuetest.	KEHTIV	T

NA-42	Arhitektuur	Rakendus peab olema jaotatud loogilisteks tehnilisteks osadeks.	Loogiline jaotus lähtub äri vajadustest, haldusest ja arendusest. Tehnilised osad peavad olema eraldi paigaldatavad.	KEHTIV	A
NA-43	Arhitektuur	Failide konverteerimised tuleb teha kasutades RIKi poolt heaks kiidetud teenuseid.		KEHTIV	A
NA-44	Arhitektuur	Kasutaja ei tohi pääseda ligi süsteemi tehnilisele informatsioonile.	Näiteks stack trace, tehnilised logid, täispikavad failinimed, kasutatavad tehnoloogiad ja raamistikud ning nende versioonid.	KEHTIV	A
NA-45	Arhitektuur	Rakendus peab olema stateless.	Peab töötama koormusjaoturiga, ei kasuta *sticky sessioneid*, SSL offload.	KEHTIV	A
NA-46	Arhitektuur	Rakenduse failide ligipääsuvajadus peab olema read-execute.	Konteinerite puhul vastutab arendaja, muul juhul administraator.	KEHTIV	A a
NA-47	Arhitektuur	Windows serverid peavad töötama windows core serveritel.		KEHTIV	A
NA-48	Arhitektuur	Andmebaasis tuleb veerutüübiks määrata selleks sisuliselt sobivaim andmetüüp.	Lähtuda andmebaasimootori dokumentatsioonist. Keelatud on kasutada (max) tüüpe, kui see pole põhjendatud ja vajalik.	KEHTIV	A
NA-49	Arhitektuur	Rakenduste masinliidestel peab olema publitseeritud tehniline spetsifikatsioon.	Näiteks SOAP WSDL ja REST OpenApi Swagger ei tohi olla publitseeritud. Tehnilises spetsifikatsioonis peavad olema: otspunkti kirjeldus, otspunkti kirjelduse väljalülitamine. Ei kehti karbitoodetele.	KEHTIV	A
NA-50	Arhitektuur	Active Directory(AD) autentimise kasutamisel peab rakendus kasutama kehtivaid standardeid.	SAML2.0 (Security Assertion Markup Language) ja ADFS (Active Directory Federation Services).	KEHTIV	A
NA-51	Arhitektuur	ID-kaardiga autentimise korral kliendipoolne veebirakendus suhtleb veebirakendusega ainult kontrollküsimuse tarbeks.	Edasine koodi täitmine ja võimalike veaolukordade töötlus peab toimuma rangelt ainult kliendi poolel. Kliendi autentimissertifikaadi kehtivus- ja autentsusekontroll teostatakse maksimaalses võimalikus mahus veebiserveri või proxy poolt. Autentimissertifikaadil on veebiserveri või proxy poolt kohustuslikult nõutav: Apache: SSLVerifyClient require; NGINX: ssl_verify_client on; Pulse TM: ssl.requireCert(); HAProxy: verify required; Tomcat: clientAuth="true"; jne… Juhul kui toimub pöördumine URL poole, kus on nõutud kliendi autentimissertifikaat ning server vastab veaga, peab klientrakendus kuvama korrektse veateate eesti keeles.	KEHTIV	A

NA-52	Arhitektuur	Robotilõksude kasutamine ja valik tuleb kooskõlastada RIK-ga.	Soovitus on robotlõkse vältida ja lahendada potentsiaalne probleem kasutades koormusjaotureid ja IP-põhiseid reegleid.	KEHTIV	A
NA-53	Arhitektuur	Rakendusetevaheline suhtlus peab olema masintöödeldav.	Üldiselt kasutame REST, SOAP(x-tee) või message queued. Muud juhud eraldi läbi rääkida Strateegia tiimiga.	KEHTIV	A
NA-54	Arhitektuur	Rakendusserverite otspunktid peavad olema piiratud ja dokumenteeritud.	Rakendus vastab ainult lubatud HTTP-meetoditele, ülejäänud annavad HTTP 405 viga.	KEHTIV	A
NA-55	Arhitektuur	Rakendusserver peab valideerima ja võimalusel verifitseerima e-posti aadresse.	Peab vastama RFC5322 ja/või RFC6854 standardile. Võimalusel peab süsteem tõendama kasutaja e-posti aadresse(verifitiseerima)	KEHTIV	A
NA-56	Arhitektuur	Rakendusel peab olema minimaalne CSP header, et funktsionaalsust tagada.	Erandid tuleb hoolikalt läbi mõelda. Väikeväärtus "self" Täiendav info: • https://csp-evaluator.withgoogle.com/ • https://www.hardenize.com/dashboards • https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-WebSocket-Accept	KEHTIV	A
NA-57	Infoturve	Kliendi ja serveri vaheline suhtlus peab kasutama TLS-protokolli.	Uusim või kehtiva toega versioon.	KEHTIV	A
NA-58	Infoturve	Andmete salvestamisel kliendi arvutisse kasutada brauseri vault-i.	Erandiks on mitmekeelse süsteemi puhul keelevalik.	KEHTIV	A
NA-59	Infoturve	Sessiooni lõpetamisel või aegumisel ei tohi kasutajal olla võimalik sessiooni värskendada või uuesti kasutada.		KEHTIV	A
NA-60	Infoturve	Andmebaasis olevate terviklikkuse turvaosaklass 2 või 3 andmete andmebaasi kirjed peab versioneerima.	Versioneerimisel peavad säilima vanad kirjed muutumatul kujul. Uue kirje tehnilistel väljadel peab olema: Kasutaja, kes kirje lõi ja loomise aeg. Kehtetuks tunnistatud kirje peab sisaldama: Kirje muutja, muutmise/kustutamise aeg.	KEHTIV	A
NA-61	Infoturve	Live andmed ei kasutata testimiseks.	Testimiseks kasutatakse sünteetilisi, genereeritud andmeid. Erindid tuleb Strateegia tiimiga eraldi kokku leppida.	KEHTIV	A
NA-62	Infoturve	Rakenduse andmebaasikontod peavad omama minimaalseid õigusi.	Rakendus ei kasuta *schema* kontot. Kontodele vajalikud õigused peavad olema kirjeldatud rakenduse installatsioonijuhendis.	KEHTIV	A
NA-63	Infoturve	Rakenduse lõppkasutajatele peavad olema õigused defineeritud läbi rollide(RBAC).	Kasutada KeyCloaki. AD OU ei tohi anda rolli.	KEHTIV	A
NA-64	Infoturve	Rakendusse ja andmebaasi ligipääsemiseks peab		KEHTIV	A

		kasutama ainult kokkulepitud dokumenteeritud autentimisprotseduure.			
NA-65	Infoturve	Salasõnad salvestatakse turvaliselt.	Krüpteering peab olema CBC, CRT vms režiimis. Kasutada ei tohi ECB režiimi. Räsi+sool+pipar osas lähtuda OWASP-i juhisest https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html	KEHTIV	A
NA-68	Infoturve	Kõik avalikud veebirakendused peavad kasutama veebitulemüüre.	IIS puhul peab kasutama näiteks URL scan, apache puhul modsecurity või vastavat tööriista. Võimalikud piirangud tuleb kokku leppida tellijaga detailanalüüsi käigus lähtuvalt tellija vajadustest ja nõudmistest. Kasutama peab whitelisting põhimõtet, mitte blacklistingut. Täiendavalt on kasutusel veebitulemüür (CloudFlare)	KEHTIV	A
NA-69	Infoturve	Rakendus peab õnnestunud sisselogimise järgselt näitama eelmise õnnestunud sisselogimise aega.	EU-direktiiv https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf	KEHTIV	A
NA-70	Infoturve	Kasutajaliidesega rakendusel peab olema esilehel rakenduse versioon.	Mõeldud on majas sees arendatud rakendusi. Rakendusserverite ja andmebaaside puhul kehtib vastupidine nõue: NA-44.	KEHTIV	A
NA-71	Infoturve	Sessioonide lõpetamine tuleb teostada serveri poolel ja kõigil rakendustel peab olema konfigureeritav kasutajasessiooni aegumise aeg.	Aeg peab olema muudetav koos teiste konfiguratsiooniparameetritega. Kui kliendilt pole etteantud aja jooksul ühtegi päringut tulnud, tuleb sessioon serveri enda algatusel lõpetada. Täiendavalt saab lugeda https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html	KEHTIV	A
NA-72	Infoturve	Kõik sisendandmed tuleb kodeerida, filtreerida ja valideerida.	Siia hulka kuuluvad vormid, masin-masin liidesed ja veebiteenused. Tuleb teha enne igasugust äriloogika täitmist.	KEHTIV	A
NA-73	Infoturve	Veebipõhiste rakenduste poolt saadetavatel vormidel peab paiknema peidetud unikaalne räsi, mida kontrollitakse vormi vastuvõtmisel.	Eesmärk on vältida CSRF rünnakuid.	KEHTIV	A
NA-74	Infoturve	Krüpteerimisel ja räsimisel tuleb lähtuda RIA uuringust.	Lähtuda viimasest dokumendist siin nimekirjas https://www.id.ee/artikkel/kruptograafiliste-algoritmide-elutsukli-uuringud-2/	KEHTIV	A
NA-75	Infoturve	Sessiooni tunnused ei tohi olla URL-st kopeeritavad.	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html	KEHTIV	A
NA-76	Infoturve	Konfiguratsioonifaile võivad muuta vaid administraatorid.	Kui rakendusel on admin liides arendatud siis seal muudatuste tegemine on OK. Muud erindid rääkida läbi strateegiatiimiga.	KEHTIV	A
NA-77	Infoturve	Kliendi sertifikaadiga rakenduse poolsel autentimisel (näiteks ID-kaart) peab rakendus vastu võtma sertifikaati HTTP päises.	Kliendi sertifikaadiga autentimisel peaks süsteem vastu võtma kliendi sertifikaati kokkulepitud päises, päise nimi peaks olema rakenduse seadistustega muudetav. Vajadus tuleneb kliendi sertifikaatide usaldusnimekirjade GLB taseme haldusest. Sertifikaat võetakse vastu kliendi veebilehitseja poolt ning edastatakse GLB'le, GLB määrab selle kokkulepitud päisesse sobivuse korral, GLB edastab juba kontrollitud sertifikaadi süsteemi kokkulepitud päises. Sama asi kehtib mistahes kliendi sertifikaadiga autentimisel ning suvalisest kohast ei tohikski süsteem sertifikaate vastu võtta.	KEHTIV	A
NA-78	Infoturve	Kõik digitembeldamist vajavad rakendused peavad kasutama		KEHTIV	A

		RIK-i digitembeldamise teenust.			
NA-79	Infoturve	Rakenduse turvalisuse tagamiseks tuleb järgida OWASP-i parimaid praktikaid.	Veebirakendus peab probleemideta läbima OWASP ASVS põhineva testi. Esmane väline turvatestimine tellitakse tellija finantseeringul. Kui selle tulemusel leitakse arendaja poolsest tegevusest või tegevusetusest põhjustatud vigu, võib tellija nõuda OWASP järeltestide kompenseerimist arendajalt. Täiendavalt saab uurida https://github.com/OWASP/ASVS	KEHTIV	A
NA-80	Arhitektuur	Rakendus peab olema optimeeritud toodangukeskkonnas toimimiseks.	Toodangukeskkonna rakendus ei tohi sisaldada osiseid, mis on ebavajalikud. NT. Debug logi, testimiseks vajalikud erisused äriloogikast. Rakendust peab olema võimalik uuesti pakendamata tarnida vabalt valitud keskkonda(arendus,test).	KEHTIV	A
NA-81	Infoturve	Ajatemplite kasutamisel eelistatakse RIK-i heaks kiidetud lahendust.	Heaks kiidetud lahenduste kohta info annab OPS-tiim.	KEHTIV	A
NA-82	Infoturve	Rakendused peavad toetama SSO kasutamist.	Sessioon peab olema *stateless*	KEHTIV	A
NA-83	Infoturve	Süsteemile määratud turvaosaklass peab olema täidetud vastavalt määruse "Võrgu- ja infosüsteemide küberturvalisuse nõuded" paragrahv 10-le.	https://www.riigiteataja.ee/akt/113122022030?leiaKehtiv Enne arenduste algust tuleb turvaosaklassist tulenevad vajadused kooskõlastada Infoturbe ja IS halduse tiimiga	KEHTIV	A
NA-86	Infoturve	Paks klient peab krüpteerima ajutised failid, mis sisaldavad delikaatseid/konfidentsiaalseid andmeid ja need sulgemisel kustutama.	Kui paks klient kasutab ajutisi faile, tuleb tagada nende perioodiline kustutamine tagamaks, et ei koormata liigselt kasutaja arvutit. Eesmärk on tagada, et rakenduse sulgemisel ei jääks kasutaja arvutisse maha informatsiooni, mida sinna jääda ei tohiks.	KEHTIV	A
NA-87	Infoturve	Rakendus peab serverist kustutama kõik ajutised failid koheselt, kui neid enam ei kasutata.	Ajutiste failide kaust peab olema konfigureeritav.	KEHTIV	A
NA-88	Infoturve	Rakendus tohib aktsepteerida ainult enda väljastatud sessioonivõtmeid.		KEHTIV	A
NA-89	Infoturve	Rakendusse üleslaetavad failid peab filtreerima, valideerima ja need peavad läbima viirusetõrje.	Tuleb teha tüübi ja faili laiendi vastavause kontroll. Failide üleslaadimise ülempiir peab olema analüüsis kirjeldatud. Filtreerimine - whitelisting, sh suurus Valideerimine - äriloogiline vastavus Viirusetõrje - Rik.Icap.VirusScanner: https://hoidla.rik.ee/#browse/browse:nuget-hosted:Rik.Icap.VirusScanner%2F1.0.0%2FRik.Icap.VirusScanner-1.0.0.nupkg Kontrollib, kas failis on viirus. Kasutamise näited: KrisDoc2 (~~KRIS-4642~~), KRIS4 (~~KRIS-4645~~), KrAvalik (~~KRIS-4643~~), KAEP (~~KRIS-4644~~) Alternatiivselt võib dll-i kompileerida lähtekoodist: https://svn.just.ee/!/#riksvn/view/head/VirusScanner/trunk	KEHTIV	A
NA-90	Infoturve	Rakendusse üleslaetava faili peab salvestama unikaalse genereeritud nimega.	Faili originaalnimi tuleb salvestada andmebaasi.	KEHTIV	A

NA-91	Infoturve	Rakendus ei tohi lubada ennast kasutada iframe sees.	Kasutada CSP headerit. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Mode https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options	KEHTIV	A
NA-92	Infoturve	Sessiooni küpsisel peavad olema turvalisuse lipud ja prefix __Host.	Sessiooni küpsise korrala tuleb lisada lipud Secure, HttpOnly ja SameSite. Küpsise nime prefiks peab olema "__Host-". Täiendav info: 1)https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie 2) https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes 3) https://owasp.org/www-community/HttpOnly 4) https://owasp.org/www-community/controls/SecureCookieAttribute 5) https://owasp.org/www-community/SameSite#:~:text=SameSite%20prevents%20the%20browser%20from,none%20%2C%20lax%20%2C%20or%20strict%20.	KEHTIV	A
NA-93	Lähtekood	Rakenduse kõik üleantavad versioonid peavad enne tellijale üle andmist olema testitud.	Testplaan ja skoop tuleb arenduse käigus tellijaga kokku leppida.	KEHTIV	A
NA-94	Logimine ja monitooring	Kriitilised sündmused - sessiooni algamine ja lõppemine ning rolli muutumine tuleb eraldi logida turvalogide tabelis.	Väliste rakenduste puhul tuleb logida kasutaja IP. Sessiooni võtmete väärtused, privaatvõtmed, kasutaja salasõnad ja muu info, mis võimaldab kasutaja isiku kindlakstegemist või on andmekaitset ohustav ei või logisse jääda.	MUUTMISEL	A
NA-95	Logimine ja monitooring	Rakendus peab logima kõiki väliste süsteemidega vahetatavaid (ka X-tee teenuste kaudu liikuvaid) pöördumisi andmevahetuslogisse.	Parim vahend on Graylog, teine valik baas, kolmas valik on faili logimine. Peab olema võimalus antud logimist välise süsteemi kaupa sisse-välja lülitada. Logi peab olema struktureeritud selliselt, et päring ja vastus on eraldi failides. Logifaili asukoht peab olema administraatori poolt ilma rakendust uuesti kompileerimata seadistatav.	KEHTIV	A
NA-98	Logimine ja monitooring	Rakendus peab logima kõiki rakenduses tekkivaid tehnilisi vigu.	Logi peab sisaldama minimaalselt aega(timestamp), veakoodi, vea sisu (komponent, stack trace, traceback vms), kogu HTTP päringut ja võimalusel kasutaja ID-d. Logimine peab olema konfigureeritav rakenduse taaskäivituseta.	KEHTIV	A
NA-99	Logimine ja monitooring	Failisüsteemi logimise korral peavad logid olema katalogiseeritud, tunnustatud faililaiendiga, roteeruvad.	Peab olema võimalus logimist välise süsteemi kaupa sisse-välja lülitada. Failisüsteemi kausta ei teki rohkem kui 10000 faili. Peab tagama, et iga rakendusserver saaks vajadusel kirjutada logid oma logifaili. Logimine peab olema konfigureeritav rakenduse taaskäivituseta.	KEHTIV	A
NA-100	Logimine ja monitooring	Rakenduse logid peavad olema ühesuguse formaadiga, masinloetavad ja täielikud.	Logiväljad, mida lõppkasutaja saab manipuleerida (IP, useragent, URL) peavad salvestuma logisse kodeeritud ja puhastatud kujul. Igas logikirjes peab olema päringu unikaalne identifikaator. Kui parameetri väärtus on tühi, tuleb see logis märkida asendusväärtusega “-”. Logi kuupäeva ja ajaformaat peab vastama ISO 8601 standardile ja olema Eesti ajavööndis.	KEHTIV	A
NA-101	Logimine ja monitooring	Logi tabelid peavad olema arhiveeritavad operatiivbaasist välja.	Tabeli suurenedes peab olema võimalik hoida vanu kirjeid, näiteks kuude või aastate kaupa, iseseisvates tabelites või teises baasis. Mehhanism peab töötama ka krüptoaheldatud logi korral.	KEHTIV	A
NA-102	Logimine ja monitooring	Kui rakendus kasutab või pakub väliseid teenuseid peab nende kohta arvestust pidama.	Peab kasutama statisikamoodulit või OpenTelemetry-t.	KEHTIV	A

NA-103	Lähtekood	Süsteem peab enne toodangusse minemist läbima jõudlustestid.	Täpne kirjeldus tuleb kokku leppida detailanalüüsi käigus. Lähtuda sellest -> https://dok.rik.ee/pages/viewpage.action?pageId=244417515	KEHTIV	A
NA-104	Logimine ja monitooring	Rakendusel peab olema masinloetav staatusleht.		KEHTIV	A
NA-106	Lähtekood	Kõik kommentaarid peavad olema põhjendatud.	Lähtekoodi kommentaarid peavad olema: 1. Kood peab olema kirjutatud selliselt, et see on loetav ka ilma kommentaarideta. Kommentaarid on mõeldud keeruliste ja/või kohendamist ja/või edasist tööd (viimaste juurde tuleks märkida TODO) vajavate kohtade jaoks. 2. Aktuaalsed - kommentaar ja kood peavad olema üksteisega vastavuses. 3. Selged ja üheselt mõistetavad. 4. Korrektselt kirjutatud - grammatika ja lauseehitus peavad olema korrektsed. 5. Andmebaasi failid ning muud koodid samadel alustel 6. Peavad olema kirjutatud eesti keeles	KEHTIV	A
NA-107	Lähtekood	Nimetused koodis peavad olema sisulised ja andma selget informatsiooni nende otstarbest.	Projekti skoobis peab olema kokku lepitud nimetamis-reeglistik.	KEHTIV	A
NA-108	Lähtekood	Koodis kasutatavad konstandid tuleb defineerida muutujatena.	Siia alla ei kuulu klassifikaatorid. Need peavad olema baasis.	KEHTIV	A
NA-109	Lähtekood	Koodis defineeritud andmetüübid peavad olema nimetava käände ainsuses. Kõik andmemassiivid tuleb nimetada nimetava mitmuses.	Näiteks "Isik", "Menetlus" jne. Andmebaasides ei tohi kasutada täpitähti. Lisainformatsioon: 1) C# - https://learn.microsoft.com/en-us/dotnet/standard/design-guidelines/general-naming-conventions 2) JAVA - https://www.oracle.com/java/technologies/javase/codeconventions-namingconventions.html 3) Python - https://peps.python.org/pep-0008/	KEHTIV	A
NA-110	Lähtekood	Andmetabelites sisalduvad võõrvõtmed peavad nime järgi seostuma tabeli ja väljaga millele need viitavad.	Näiteks kui on tegu tabelitega 'Isik' ja 'Auto', siis seos 'isik_auto' oleks: Isik.ID=Auto.Isik_ID	KEHTIV	A
NA-111	Lähtekood	Andmebaasi väljade pikkused peavad lähtuma analüüsis kirjeldatud nõuetest.	Tuleb meeles pidada, et 1 byte ei pruugi võrduda 1 tähemärgiga, näiteks täpitähed.	KEHTIV	A
NA-115	Lähtekood	Koodi valideerimiseks kasutame SonarQube reegleid.	Koos SonarQube-ga peab tegema ka Trivy skaneerimise.	KEHTIV	A
NA-118	Lähtekood	Lähtekoodis ei tohi olla mitte kasutatavaid osasid.		KEHTIV	A
NA-120	Lähtekood	Koodibaasis olevad ärilised terminid peavad olema eesti keeles.	Ärianalüüs ja kood peavad teineteist peegeldama. Ka andmebaasis olevad nimetused peavad olema eesti keeles.	KEHTIV	A
NA-121	Andmekvaliteet ja standardid	Aadressiandmete käitlemisel lähtuda määrusest "Aadressiandmete süsteem."	Kasutada ADS-i. Link määrusele https://www.riigiteataja.ee/akt/128122024043	KEHTIV	A

NA-123	Infoturve	Iga transaktsiooni juures tuleb kontrollida kasutaja õiguseid ja rollikuuluvust.	OWASP nõuetest -> "Validate the Permissions on Every Request" https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html#validate-the-permissions-on-every-request	KEHTIV	A
NA-124	Andmekvaliteet ja standardid	Tegevusalade käitlemisel lähtuda määrusest "Klassifikaatorite süsteem."	Kasutada RIK EMTAK teenust. https://www.riigiteataja.ee/akt/12910889	KEHTIV	A
NA-126	Infoturve	Süsteemist väljaminevad veateated ei tohi sisaldada süsteemiinfot.	Näiteks: "Tekkis tehniline viga. Päringu ID: XXXXX". Reaalne veateade peab logis säilima!	KEHTIV	A
NA-127	Dokumentatsioon	Kogu rakenduse dokumentatsioon peab olema kirjutatud eesti keeles.	Erandiks kolmandate osapoolte komponendid.	KEHTIV	A
NA-128	Dokumentatsioon	Dokumentatsioon peab vastama RIK dokumentatsiooniplaani nõuetele.	https://dok.rik.ee/pages/viewpage.action?pageId=190751639	KEHTIV	A
NA-129	Dokumentatsioon	Iga uue versiooniga käib kaasas muudatuste kirjeldus.	*Changelog* või *release notes*.	KEHTIV	A
NA-130	Versioneerimine	Kõik rakenduse testimiseks, koolituseks või implementeerimiseks üle antavad tarkvarapaketid peavad asuma RIK koodihoidlas.	Arendajale antakse selleks õigused RIK-i koodihoidlas.	KEHTIV	A
NA-133	Versioneerimine	Peab kasutama RIK piletihalduskeskkonda.	Kasutusel on JIRA. Kaasa arvatud välised osapooled.	KEHTIV	A
NA-137	Versioneerimine	Kolmanda osapoole teegid peavad asuma RIK-i hoidlas.	hoidla.rik.ee	KEHTIV	A
NA-138	Versioneerimine	Andmebaasi skriptide sisu peab olema kontrollitav.	Administraator peab saama veenduda skriptide sisus.	KEHTIV	A

118 issues Refresh

Lisad:
Lisa 1.1.1 – Staatuslehe näidis

No labels