Siseministeeriumi infotehnoloogia- ja arenduskeskus

KÄSKKIRI

Tallinn 08.07.2025 nr 1-1/109

Siseministeeriumi infotehnoloogia- ja arenduskeskuse ISO/IEC 27001:2022 kohaldusmäärang

Siseministri 17. veebruari 2020 määruse nr 8 „Siseministeeriumi infotehnoloogia- ja arenduskeskuse põhimäärus“ § 10 lg 2 alusel:

1. Kehtestan käskkirja lisaks oleva Siseministeeriumi infotehnoloogia- ja arenduskeskuse ISO/IEC 27001:2022 kohaldusmäärangu.

2. Käskkiri jõustub allkirjastamise hetkest.

3. Panen kontrolli käskkirja täitmise üle SMITi riskijuhile.

LISAD:

Lisa 1: Siseministeeriumi infotehnoloogia- ja arenduskeskuse ISO/IEC 27001:2022 kohaldusmäärang

(allkirjastatud digitaalselt)

Mart Nielsen
peadirektor

Lisa 1. Siseministeeriumi infotehnoloogia- ja arenduskeskuse ISO/IEC 27001:2022 kohaldusmäärang

Identifikaator	Meetme nimetus	Meetme kirjeldus	Alus/viide	Kas meede kohaldub?	Kas meede on teostatud?
5	**Korraldusmeetmed**				
5.1	Infoturvapoliitikad	Tuleks määratleda, juhtkonnas kinnitada, avaldada, teatada ja teadvustada asjakohasele personalile ja asjakohastele huvipooltele infoturvapoliitika ja teemapoliitikad ning vaadata need läbi plaaniliste vaheaegade järel ja suuremate muudatuste toimumisel.	RISKREG-6 RISKREG-8	JAH	JAH
5.2	Infoturberollid ja -kohustused	Vastavalt organisatsiooni vajadustele tuleks määratleda ja kinnistada infoturberollid ja kohustused.	RISKREG-22	JAH	JAH
5.3	Kohustuste lahusus	Vastuolus olevad ülesanded ja vastuolus olevad vastutusalad tuleks lahutada.	RISKREG-23 RISKREG-52	JAH	JAH
5.4	Juhtkonna kohustused	Juhtkond peaks nõudma, et kogu personal rakendaks infoturvet vastavalt kehtestatud infoturvapoliitikale, teemapoliitikatele ja organisatsiooni protseduuridele.	RISKREG-31	JAH	JAH
5.5	Kontakt ametivõimudega	Organisatsioon peaks looma kontakti ametivõimudega ja seda säilitama.	RISKREG-24	JAH	JAH
5.6	Kontakt erihuvirühmadega	Organisatsioon peaks looma kontakti erihuvirühmadega või spetsialistide turvafoorumitega ja kutseühingutega ning seda säilitama.	RISKREG-25	JAH	JAH
5.7	Ohuluure	Tuleks koguda teavet infoturvaohtude kohta ja analüüsida seda ohuteabe saamiseks.	RISKREG-25	JAH	JAH
5.8	Infoturve projektihalduses	Projektihaldusse tuleks integreerida infoturve.	RISKREG-26 RISKREG-88	JAH	JAH
5.9	Teabe ja kaasnevate varade inventariloend	Tuleks koostada teabe ja muude varade ning nende omanike loend ja seda hooldada.	RISKREG-34	JAH	JAH
5.10	Teabe ja kaasnevate varade lubatav kasutamine	Tuleks piiritleda, dokumenteerida ja teostada teabe ja kaasnevate muude varade lubatava kasutamise reeglid ja käitlusprotseduurid.	RISKREG-35 RISKREG-39	JAH	JAH

5.11	Varade tagastamine	Töötajad ja kõik muud ajaomased huvipooled peaksid oma töösuhte, lepingu või kokkuleppe muutumisel või lõppemisel tagastama kõik nende käes olevad organisatsiooni varad.	RISKREG-36	JAH	JAH
5.12	Teabe turvaliigitus	Teave tuleks vastavalt organisatsiooni infoturvavajadustele liigitada konfidentsiaalsuse, tervikluse, käideldavuse ja asjasse puutuvate kolmandapoolsete nõuete põhjal.	RISKREG-37	JAH	JAH
5.13	Teabe märgistus	Tuleks välja töötada ja teostada sobiv teabe märgistuse protseduuristik vastavalt organisatsioonis kasutusele võetud liigitusskeemile.	RISKREG-38	JAH	JAH
5.14	Teabe edastuse turve	Organisatsioonis ning organisatsiooni ja muude poolte vahel peaksid igat tüüpi edastusvahendite kohta olema kasutusel teabe edastuse reeglid, protseduurid või kokkulepped.	RISKREG-85 RISKREG-86	JAH	JAH
5.15	Pääsu reguleerimine	Tegevusalaste ja infoturbenõuete põhjal tuleks kehtestada ja teostada reeglid juurdepääsuks teabele ja muudele kaasnevatele varadele.	RISKREG-43 RISKREG-45	JAH	JAH
5.16	Identiteedi-haldus	Hallata tuleb identiteetide kogu elutsüklit.	RISKREG-482	JAH	JAH
5.17	Autentimis-teave	Autentimisteabe kinnistamist ja haldust tuleks reguleerida haldusprotsessiga, mis sisaldaks ka personali nõustamist autentimisteabe asjakohase käitluse alal.	RISKREG-44 RISKREG-48 RISKREG-51	JAH	JAH
5.18	Pääsuõiguste haldus	Õigusi juurdepääsuks teabele ja muudele kaasnevatele varadele tuleks anda, läbi vaadata, muuta ja kõrvaldada vastavalt organisatsiooni pääsu reguleerimise teemapoliitikale ja reeglitele.	RISKREG-46 RISKREG-47 RISKREG-99	JAH	JAH
5.19	Tarnesuhete infoturve	Tuleks määratleda ja teostada protsessid ja protseduurid tarnija toodete või teenuste kasutamisega kaasnevate infoturvariskide käsitluseks.	RISKREG-98 RISKREG-252 RISKREG-265 RISKREG-520	JAH	JAH

5.20	Infoturbe käsitlus tarnelepetes	Sõltuvalt tarnijasuhte tüübist tuleks kehtestada ja iga tarnijaga kokku leppida asjakohased infoturvanõuded.	RISKREG-98	JAH	JAH
5.21	IKT tarneahela infoturbe haldus	IKT-toodete ja -teenuste tarneahela infoturvariskide halduseks tuleks määratleda ja teostada protsessid ja protseduurid.	RISKREG-99	JAH	JAH
5.22	Tarnija teenuste seire, läbivaatus ja muudatuste haldus	Organisatsioon peaks regulaarselt seirama, läbi vaatama, hindama ja haldama muudatusi tarnija infoturbe tavades ja teenuseväljastuses.	RISKREG-100 RISKREG-101	JAH	JAH
5.23	Pilvteenuste kasutamise infoturve	Tuleks rajada protsessid pilvteenuste hankimiseks, kasutamiseks, halduseks ja hülgamiseks kooskõlas organisatsiooni infoturvanõuetega.	RISKREG-472 RISKREG-473 RISKREG-486	JAH	JAH
5.24	Infoturvaintsidentide halduse kavandamine ja ettevalmistus	Organisatsioon peaks kavandama ja ette valmistama infoturvaintsidentide haldust, määratledes, kehtestades ja teatavaks tehes infoturvaintsidentide halduse protsessid, rollid ja kohustused.	RISKREG-102	JAH	JAH
5.25	Infoturvaintsidentide hindamine ja otsustamine	Organisatsioon peaks hindama infoturvasündmusi ja otsustama, kas need tuleb liigitada infoturvaintsidentideks.	RISKREG-88 RISKREG-104	JAH	JAH
5.26	Infoturvaintsidentidele reageerimine	Infoturvaintsidentidele tuleks reageerida vastavalt selleks dokumenteeritud protseduuridele.	RISKREG-105	JAH	JAH
5.27	Infoturvaintsidentidest õppimine	Infoturvameetmete tugevdamiseks ja täiustamiseks tuleks kasutada infoturvaintsidentidest saadud teadmust.	RISKREG-106	JAH	JAH
5.28	Asitõendite kogumine	Organisatsioon peaks kehtestama ja teostama protseduurid infoturva-sündmustega seotud asitõendite kogumiseks, hõiveks ja säilitamiseks.	RISKREG-107	JAH	JAH
5.29	Infoturve halvangu ajal	Organisatsioon peaks kavandama, kuidas halvangu ajal säilitada teabe turvalisus sobival tasemel.	RISKREG-474	JAH	JAH
5.30	IKT valmisolek jätkusuutlikkuseks	Tegevuse jätkuvuse eesmärkide ja IKT jätkuvuse nõuete põhjal	RISKREG-108 RISKREG-	JAH	JAH

		kavandada, teostada, säilitada ja testida IKT valmidus.	109 RISKREG-121		
5.31	Õigusaktide ja lepingute nõuded	Tuleks piiritleda, dokumenteerida ja ajakohastada teabe turvalisust puudutavad õiguslikud, põhikirjalised, regulatiivsed ja lepingulised nõuded ning organisatsiooni meetodid nende nõuete täitmiseks.	RISKREG-111 RISKREG-115	JAH	JAH
5.32	Intellektuaal-omandiõiguste kaitse	Intellektuaalomandiõiguste kaitseks peaks organisatsioon teostama sobivad protseduurid.	RISKREG-112	JAH	JAH
5.33	Andmike kaitse	Andmikke tuleks kaitsta kaotamise, hävimise, võltsimise, lubamatu juurdepääsu ja lubamatu avaldamise eest.	RISKREG-113	JAH	JAH
5.34	Privaatsus ja isikustatud teabe kaitse	Organisatsioon peaks piiritlema privaatsuse säilitamise ja isikuteabe kaitse nõuded vastavalt kohaldatavatele õigusaktidele, eeskirjadele ja lepingunõuetele.	RISKREG-114	JAH	JAH
5.35	Infoturbe sõltumatu läbivaatus	Organisatsiooni meetodeid infoturbe halduseks ja nende teostust, sealhulgas inimesi, protsesse ja tehnoloogiaid tuleks plaaniliste vaheaegade järel või oluliste muudatuste korral sõltumatult läbi vaadata.	RISKREG-116	JAH	JAH
5.36	Vastavus infoturvapoliitikatele, -eeskirjadele ja standarditele	Vastavust organisatsiooni infoturvapoliitikale, teemapoliitikatele, reeglitele ja standarditele tuleks regulaarselt läbi vaadata.	RISKREG-116 RISKREG-117	JAH	JAH
5.37	Dokumenteeritud tööprotseduurid	Infotöötlusvahendite tööprotseduurid tuleks dokumenteerida ja teha kättesaadavaks neid vajavale personalile.	RISKREG-69	JAH	JAH
6	**Personalimeetmed**				
6.1	Taustakontroll	Kõigi töötajaks kandideerijate tausta tuleks kontrollida enne nende liitumist organisatsiooniga ja jooksvalt, võttes arvesse kohaldatavad õigusaktid, eeskirjad ja eetikanormid ning proportsionaalsuse tegevusalaste nõuetega, taotletava teabe	RISKREG-29	JAH	JAH

		liigimääranguteg a ja tajutud riskidega.			
6.2	Töölepingu sätted	Töölepingud peaksid sätestama töötaja ja organisatsiooni infoturvakohustused.	RISKREG-30	JAH	JAH
6.3	Infoturvateadlikkus, -haridus ja -koolitus	Organisatsiooni ja asjasse puutuvate huvipoolte personal peaks saama sobiva infoturvateadvustuse, -hariduse ja -koolituse ning oma tööülesandeid puudutavad organisatsiooni infoturvapoliitika, teemapoliitikate ja protseduuride ajakohastused.	RISKREG-32	JAH	JAH
6.4	Distsiplinaarprotsess	Infoturvapoliitikat rikkunud personalile ja muudele asjasse puutuvatele huvipooltele sanktsioonide rakendamiseks tuleks formaliseerida ja teatavaks teha mingi distsiplinaarprotsess.	RISKREG-33	JAH	JAH
6.5	Kohustused pärast töösuhte lõppu või muudatust	Tuleks määratleda, jõustada ning asjasse puutuvaile töötajaile ja muudele huvipooltele teatavaks teha need infoturbekohustused ja -ülesanded, mis jäävad kehtima pärast töösuhte lõppu või muutumist.	RISKREG-30	JAH	JAH
6.6	Konfidentsiaalsuslepped	Tuleks piiritleda, dokumenteerida ja regulaarselt läbi vaadata konfidentsiaalsuslepped, mis kajastavad organisatsiooni teabe kaitse vajadusi, ning võtta neile allkirjad personalilt ja muudelt asjasse puutuvatelt huvipooltelt.	RISKREG-260	JAH	JAH
6.7	Kaugtöö turve	Personali kaugtöö puhul tuleb väljaspool organisatsiooni territooriumi taotletava, töödeldava või talletatava teabe kaitseks rakendada turvameetmed.	RISKREG-28	JAH	JAH
6.8	Infoturvasündmustest teatamine	Organisatsioon peaks rakendama mehhanismi, millega töötajad saaksid sobivate kanalite kaudu aegsasti teatada ilmnenud või oletatavatest infoturvasündmustest.	RISKREG-102 RISKREG-103 RISKREG-122	JAH	JAH
7	**Füüsilised meetmed**				

7.1	Füüsilised turvaperimeet-rid	Teavet ja kaasnevaid muid varasid sisaldavate alade kaitseks tuleks määratleda turvaperimeetrid ja kasutada neid.	RISKREG-56	JAH	JAH
7.2	Füüsilise sisenemise piiramine	Turvalised alad tuleks kaitsta asjakohaste pääsumeetmete ja pääsupunktidega.	RISKREG-57 RISKREG-59	JAH	JAH
7.3	Kabinettide, ruumide ja rajatiste turve	Tuleks kavandada ja teostada kabinettide, ruumide ja rajatiste turve.	RISKREG-58	JAH	JAH
7.4	Füüsilise turbe seire	Territooriumi tuleks pidevalt seirata lubamatu füüsilise pääsu avastamiseks.	RISKREG-58	JAH	JAH
7.5	Kaitse füüsiliste ja keskkonna-ohtude eest	Tuleks kavandada ja ellu viia kaitse füüsiliste ja keskkonnaohtude, näiteks loodusõnnetuste ning muude tahtlike või ettekavatsematute füüsiliste taristuohtude eest.	RISKREG-58	JAH	JAH
7.6	Töökorraldus kaitstud aladel	Tuleks kavandada ja teostada turvalistel aladel töötamise turvameetmed.	RISKREG-58	JAH	JAH
7.7	Tühi laud ja tühi ekraan	Tuleks luua ja sobivalt jõustada tühja laua poliitika paberdokumentide ja salvestuskandjate kohta ning tühja ekraani poliitika infotöötlusvahendite kohta.	RISKREG-68	JAH	JAH
7.8	Seadmete paigutus ja kaitse	Seadmed tuleks paigutada turvaliselt ja kaitstult.	RISKREG-61	JAH	JAH
7.9	Territooriumi-väline varade turve	Territooriumivälised varad tuleks kaitsta.	RISKREG-66	JAH	JAH
7.10	Salvestuskand-jate turve	Salvestuskandjaid tuleks hallata kogu nende elutsükli (soetamine, kasutus, transport, kõrvaldamine) kestel, kooskõlas organisatsiooni liigitusskeemi ja käitlusnõuetega.	RISKREG-40 RISKREG-41 RISKREG-42 RISKREG-65	JAH	JAH
7.11	Tehnoteenuste turve	Infotöötlusvahendid tuleks kaitsta elektrikatkestuste ja tehnoteenuste muudest tõrgetest tingitud katkestuste eest.	RISKREG-62	JAH	JAH
7.12	Kaabelduse turve	Elektri-, andme- ja tugiteabeteenuste kaablid tuleks kaitsta infopüügi, häiringute ja kahjustuste eest.	RISKREG-63	JAH	JAH
7.13	Seadmete hooldus	Teabe käideldavuse, tervikluse ja konfidentsiaalsuse	RISKREG-64	JAH	JAH

		tagamiseks tuleks seadmeid korralikult hooldada.			
7.14	Seadmete turvaline kõrvaldamine või taaskasutus	Tuleks kontrollida, kas salvestuskandjaid sisaldavatest seadmetest on enne kõrvaldamisele või taaskasutusse suunamist eemaldatud tundlik teave ja litsentstarkvara.	RISKREG-67	JAH	JAH
8	**Tehnilised meetmed**				
8.1	Kasutaja lõppseadmete turve	Teave, mida talletatakse või töödeldakse kasutaja lõppseadmetes või millele juurdepääs toimub nende kaudu, tuleks kaitsta.	RISKREG-27 RISKREG-66 RISKREG-475	JAH	JAH
8.2	Eelispääsuõiguste piiramine	Eelispääsuõiguste andmist ning kasutamist tuleks piirata ja hallata.	RISKREG-44	JAH	JAH
8.3	Teabepääsu piiramine	Juurdepääs teabele ja kaasnevatele muudele varadele tuleks piirata kooskõlas pääsu reguleerimise kehtiva teemapoliitikaga.	RISKREG-49	JAH	JAH
8.4	Lähtekoodi kaitse	Lugemis- ja kirjutamispääsu lähtekoodi, arendusvahendite ja tarkvarateekide juurde tuleks asjakohaselt hallata.	RISKREG-53 RISKREG-124	JAH	JAH
8.5	Turvaline autentimine	Teabepääsu piirangute ja pääsu reguleerimise teemapoliitikate põhjal tuleks teostada turvalised autentimis-tehnoloogiad ja -protseduurid.	RISKREG-50	JAH	JAH
8.6	Suutvuse haldus	Ressursikasutust tuleks seirata ja korrigeerida kooskõlas praeguste ja oodatavate suutvusnõuetega.	RISKREG-71	JAH	JAH
8.7	Kahjurvaratõrje	Tuleks rakendada kahjurvaratõrje ja toetada seda kasutajate asjakohase teadlikkusega.	RISKREG-73	JAH	JAH
8.8	Tehniliste nõrkuste haldus	Tuleks hankida teavet kasutusel-olevate infosüsteemide tehniliste nõrkuste kohta. Tuleks hinnata organisatsiooni ohustatust sellistest nõrkustest ning rakendada kohased meetmed.	RISKREG-80	JAH	JAH
8.9	Konfiguratsioonihaldus	Riistvara, tarkvara, teenuste ja võrkude konfiguratsioonid, sealhulgas turvakonfiguratsioonid, tuleks kehtestada, dokumenteerida, rakendada, seirata ja läbi vaadata.	RISKREG-476	JAH	JAH

8.10	Teabe kustutus	Talletatud teave, mida enam ei vajata, tuleks infosüsteemidest, seadmetest ja muudelt salvestuskandjatelt kustutada.	RISKREG-477	JAH	JAH
8.11	Andmete varjamine	Kooskõlas organisatsiooni pääsureguleerimise teemapoliitikaga ja muude kaasnevate teemapoliitikatega, samuti tegevusnõuetega tuleks kasutada andmete varjamist, arvestades kohaldatavaid õigusakte.	RIKSREG-478	JAH	JAH
8.12	Andmelekete vältimine	Süsteemides, võrkudes ja kõigis tundlikke andmeid töötlevates, talletavates või edastatavates muudes seadmetes tuleks rakendada andmelekete vältimise abinõusid.	RISKREG-479	JAH	JAH
8.13	Teabe varundamine	Teabe, tarkvara ja süsteemide varukoopiaid tuleks säilitada ja regulaarselt testida kooskõlas varunduse kokkulepitud teemapoliitikaga.	RISKREG-74	JAH	JAH
8.14	Infotöötlus-vahendite liiasus	Infotöötlusvahendid tuleks teostada käideldavusnõuete täitmiseks piisava liiasusega.	RISKREG-108 RISKREG-110	JAH	JAH
8.15	Logimine	Erindite, tõrgete ja muude asjasse puutuvate sündmuste kohta tuleks genereerida logid ning need säilitada, kaitsta ja analüüsida.	RISKREG-76 RISKREG-77	JAH	JAH
8.16	Seiretegevused	Võrke, süsteeme ja rakendusi tuleks anomaalse käitumise avastamiseks seirata ning teha asjakohased toimingud potentsiaalsete infoturvaintsi-dentide hindamiseks.	RISKREG-480	JAH	JAH
8.17	Kellade sünkroniseeri-mine	Organisatsioonis kasutatavate infotöötlussüsteemide kellad tuleks sünkroniseerida heakskiidetud ajaallikatega.	RISKREG-78	JAH	JAH
8.18	Privileeg-utiliitide kasutamise haldus	Tuleks piirata ja rangelt ohjata selliste utiliitide kasutamist, mis on võimelised eirama süsteemi ja rakenduste piiranguid.	RISKREG-52	JAH	JAH
8.19	Tarkvara turvaline installimine	Töösüsteemidele tarkvara installimise turvaliseks halduseks tuleks teostada protseduurid ja meetmed.	RISKREG-79	JAH	JAH
8.20	Võrkude turve	Teabe kaitseks süsteemides ja rakendustes tuleks võrku ja võrguseadmeid turvata, hallata, ja reguleerida.	RISKREG-82	JAH	JAH

8.21	Võrguteenuste turve	Võrguteenuste turvamehhanismid, teenusetasemed ja teenusenõuded tuleks piiritleda, rakendada ja allutada seirele.	RISKREG-83	JAH	JAH
8.22	Võrkude lahusus	Infoteenuste, kasutajate ja infosüsteemide rühmad organisatsiooni võrkudes peaksid olema lahus.	RISKREG-84	JAH	JAH
8.23	Veebi filtreerimine	Kahjursisule avatuse vähendamiseks tuleks hallata pöördumist välissaitide poole.	RISKREG-481	JAH	JAH
8.24	Krüptograafia kasutamine	Tuleks määratleda ja teostada reeglid krüptograafia toimivaks kasutamiseks, sealhulgas krüptovõtmete halduseks.	RISKREG-54 RISKREG-55	JAH	JAH
8.25	Turvaline arenduse elutsükkel	Tuleb kehtestada ja rakendada reeglid tarkvara ja süsteemide turvaliseks arenduseks.	RISKREG-88	JAH	JAH
8.26	Rakenduste turvanõuded	Rakenduste väljatöötamisel või hankimisel tuleks piiritleda, spetsifitseerida ja kinnitada infoturvanõuded.	RISKREG-88	JAH	JAH
8.27	Turvalise süsteemiarhitektuuri ja tehnostuse põhimõtted	Kõigile infosüsteemide arendustegevustele tuleks kehtestada, dokumenteerida, hooldada ja rakendada turvaliste süsteemide tehnostuse põhimõtted.	RISKREG-92	JAH	JAH
8.28	Turvaline kodeerimine	Tarkvaraarendusele tuleks rakendada turvalise kodeerimise põhimõtteid.	RISKREG-470	JAH	JAH
8.29	Turvatestimine arenduse ja vastuvõtmise käigus	Arenduse elutsüklis tuleks määratleda ja teostada turvatestimise protsessid.	RISKREG-95 RISKREG-96	JAH	JAH
8.30	Väljastarenduse turve	Organisatsioon peaks väljasttellitud süsteemiarendusse puutuvaid tegevusi suunama, seirama ja läbi vaatama.	RISKREG-94	JAH	JAH
8.31	Arendus-, testimis- ja tarbekeskkondade lahusus	Arendus-, testimis- ja tarbekeskkonnad peavad olema lahus ja turvalised.	RISKREG-72 RISKREG-93	JAH	JAH
8.32	Muudatuste haldus	Infotöötlusvahendite ja infosüsteemide muudatused tuleks allutada muudatusehalduse protseduuridele.	RISKREG-70 RISKREG-89 RISKREG-91	JAH	JAH
8.33	Testteave	Testteavet tuleks hoolikalt valida, kaitsta ja hallata.	RISKREG-97	JAH	JAH
8.34	Infosüsteemide kaitse audittestimisel	Audittestid ja muud töösüsteemide hindamist sisaldavad tõendustegevused	RISKREG-81	JAH	JAH

		tuleks kavandada ning testija ja asjakohase juhtkonna vahel kokku leppida.			