KUTSESTANDARD

IT-turvaspetsialist, tase 5

Kutsestandard on dokument, milles kirjeldatakse tööd ning töö edukaks tegemiseks vajalike oskuste, teadmiste ja hoiakute kogumit ehk kompetentsusnõudeid. Kutsestandardeid kasutatakse õppekavade koostamiseks ja kutse andmiseks.

Kutsenimetus	Eesti kvalifikatsiooniraamistiku (EKR) tase
IT-turvaspetsialist, tase 5	5

A-osa
KUTSEKIRJELDUS

A.1 Töö kirjeldus
IT-turvaspetsialist rakendab organisatsiooni IKT turvapoliitikat ja parimaid praktikaid, pakub välja ja rakendab vajalikud turvalisuse kontrollimehhanismid, juhendab, toetab ja informeerib kaastöötajaid, et tagada IKT turvaline toimimine. IT-turvaspetsialist töötab tavaliselt asutuses, kus IKT süsteemid moodustavad olulise osa asutuse varadest, äriprotsessid sõltuvad IKT süsteemidest ja rakendustest, äriandmeid kogutakse ja juhitakse IKT süsteemide kaudu. 5. taseme IT-turvaspetsialist töötab erinevate IKT süsteemide ja tööriistadega. Ta juhendab kaastöötajaid ja väikest meeskonda, kui see on vajalik. IT-turvaspetsialisti kutse kirjeldamise aluseks on Euroopa IKT-kompetentside raamistik (e-CF), mis määratleb kokku 40 põhikompetentsi. e-CF raamistik on leitav veebilehel www.ecompetences.eu.
A.2 Tööosad
1. Sisendi andmine IKT rakenduse projekteerimisse/kavandamisse (e-CF kompetents A.6.) 2. Tehnoloogia arengu jälgimine (e-CF kompetents A.7.) 3. Süsteemide integreerimine (e-CF kompetents B.2.) 4. Kliendile pakutava toote testimine (e-CF kompetents B.3.) 5. Lahenduse paigaldamine (e-CF kompetents B.4.) 6. Dokumentatsiooni koostamine (e-CF kompetents B.5.) 7. Kasutajatugi (e-CF kompetents C.1.) 8. Muudatuste tugi (e-CF kompetents C.2.) 9. Teenuse osutamine (e-CF kompetents C.3.) 10. Probleemihaldus (e-CF kompetents C.4.) 11. Infoturbestrateegia väljatöötamises osalemine (e-CF kompetents D.1.) 12. Personaliarendus (e-CF kompetents D.9.) 13. Riskihaldus (e-CF kompetents E.3.) 14. Infoturbe haldamine (e-CF kompetents E.8.)
A.3 Töö keskkond ja eripära
Tavaliselt töötab IT-turvaspetsialist väikeettevõttes iseseisva IT-turvaspetsialistina või suures ettevõttes IT infoturbe meeskonnas. 5. taseme IT-turvaspetsialist töötab väga kiiresti muutuvate tehnoloogiate keskkonnas. Töö on perioodiliti kiire ja pingeline.
A.4 Töövahendid
Operatsioonisüsteemid, turbetarkvara, protsesside kirjelduse ja projekteerimise tööriistad, tarkvara arendamise tööriistad, tunnustatud infoturbe raamistikud ja standardid.
A.5 Tööks vajalikud isikuomadused
IT-turvaspetsialisti töö eeldab loogilist mõtlemist, analüüsivõimet, algatusvõimet, kohusetundlikkust, seaduskuulekust, keskendumisvõimet, võimet töötada metoodiliselt ja olla detailidele orienteeritud.

A.6 Kutsealane ettevalmistus
IT-turvaspetsialistil on vähemalt keskharidus ning varasemalt (kutseõppe tasemeõppes, IKT-alasel täiendkoolitusel või töökohal) omandatud 4.taseme IT-süsteemide spetsialisti kompetentsid.
A.7 Enamlevinud ametinimetused
IT-süsteemide spetsialist, IT-turvaspetsialist, küberturbe spetsialist, IKT-turbespetsialist, IKT turvalisuse konsultant, küberturvalisuse konsultant.

B-osa
KOMPETENTSUSNÕUDED

B.1 Kutse struktuur
IT-turvaspetsialisti kutse taotlemisel tuleb tõendada kõik kompetentsid (B.2.1-B.2.15).

B.2 Kompetentsid

KOHUSTUSLIKUD KOMPETENTSID

B.2.1 Sisendi andmine IKT rakenduse projekteerimisse/kavandamisse (e-CF A6)	EKR tase 5
Tegevusnäitajad 1. Osaleb organisatsiooni äriprotsesside turvalisuse tagamises, sh uute rakenduste kavandamises ning olemasolevate uuendamises. 2. Sõnastab kavandatava süsteemi turvanõuded ja turvatingimused, aitab koostada süsteemi mittefunktsionaalnõudeid (NFR). 3. Pärast süsteemi teostamist verifitseerib nõuete täidetuse (ülevaatuse ja testimise teel).	
B.2.2 Tehnoloogia arengu jälgimine (e-CF A7)	**EKR tase 5**
Tegevusnäitajad 1. Hoiab end kursis IT-alaste uudiste ja tehnoloogiliste uuendustega, samuti turvanõrkuste, andmelekete ning krüptograafia alaste uudistega, värskete turvaohtude ja kaitsemeetoditega; jälgib uudiskirju, ohukirjelduste vooge ning muid organisatsiooni infoturbe jaoks olulisi teabekanaleid. 2. Teavitab IT-meeskonda ja vajadusel juhtkonda talle teatavaks saanud ning äri mõjutada võivatest turvakeskkonna muutustest.	
B.2.3 Komponentide integreerimine süsteemi (e-CF B2)	**EKR tase 5**
Tegevusnäitajad 1. Paigaldab infoturvet tagavad või parendavad seadmed, tarkvara või alamsüsteemi komponendid käitatavasse või evitatavasse süsteemi, järgib seejuures infoturbe head tava ning muudatustehalduse protseduure. 2. Teeb süsteemist või selle osast varukoopiad, tagab süsteemi tervikluse integratsiooniprotsessis. 3. Testib evitatud süsteemiosa funktsionaalset toimimist ja jõudlust. 4. Koostöös IT meeskonnaga tagab paigaldatud süsteemi, riistvara, tarkvara või komponendi jätkuva turvalisuse (andmete konfidentsiaalsuse ja tervikluse ning süsteemi käideldavuse).	
B.2.4 Kliendile pakutava toote testimine (e-CF B3)	**EKR tase 5**
Tegevusnäitajad 1. Koostab ja hindab IKT süsteemide testimise protseduure (sh eelmisele versioonile naasmise protseduure) ning sooritab testimist nende protseduuride alusel, arvestades infoturvanõudeid, testimisprotsessi elutsüklit ning testimise liike. 2. Hindab infoturbe aspektist toote kasutatavust, jõudlust, töökindlust ja ühilduvuse aspekte ettevõttesiseste ja -väliste, riigisiseste ja rahvusvaheliste standardite valguses. 3. Koostab töödokumente ja -aruandeid, vajadusel tõendab infoturvameetmete ja IT-lahenduse vastavust infoturbealastele sertifitseerimisnõuetele. 4. Osaleb toote läbistustestimise korraldamisel turvalisuse parendamise eesmärgil.	

B.2.5 Lahenduse paigaldamine (e-CF B4)	EKR tase 5
Tegevusnäitajad 1. Plaanib ja organiseerib paigaldamise ja seadistamise, arvestades evituse ja olemasoleva arhitektuuri koosmõju. 2. Koostöös IT meeskonnaga, seadistab paigaldatud süsteemi (sh võrk, serverid, andmebaasid, veeb ja pilv) vastavalt turvanõuetele. 3. Kaasab täiendavaid erialaseid ressursse, nt väliseid võrguteenustajaid. 4. Võimalusel kasutab innovatiivseid lahendusi ning integreerib neid olemasolevatesse süsteemidesse ja teenustesse, arvestades turvameetmeid. 5. Annab kasutajale üle täielikult töökorras lahenduse (sh dokumentatsiooni), lähtudes tarkvara pakendamise ja levitamise nõuetest.	
B.2.6 Dokumentatsiooni koostamine (e-CF B5)	**EKR tase 5**
Tegevusnäitajad 1. Koostab tooteid, teenuseid, komponente või rakendusi kirjeldavaid dokumente (sh kasutusjuhendeid). 2. Toodete, rakenduste ja teenuste projekteerimisel, väljatöötamisel ja juurutamisel juhindub kõigist selleks vajalikest dokumentidest. 3. Dokumenteerimisel kasutab versioonihaldust, järgib tehnilise dokumenteerimise tavasid ja keelekasutust (sh EVS 8). 4. Dokumentide tutvustamisel sihtgrupile valib asjakohase stiili ja suhtluskanali (nt esitlus, netivideo, dokumendivormis kasutusjuhend). 5. Tagab kirjeldatava objekti funktsionaalsuste ja omaduste nõuetekohase dokumenteerimise. 6. Tagab oma vastutusala dokumentide ajakohasuse ja kehtivuse. 7. Vajadusel kehtestab oma vastutusalas dokumenteerimisnõuded.	
B.2.7 Kasutajatugi (e-CF C1)	**EKR tase 5**
Tegevusnäitajad 1. Vastab kasutajate infoturbealastele küsimustele ja päringutele, registreerib asjakohase teabe. 2. Tuvastab turvaprobleemi olemuse küsitledes kasutajaid, analüüsides sümptomeid ning kasutades asjakohaseid IT tugirakendusi. 3. Otsib lahendusi kasutajatel esinenud turvaprobleemidele, kasutades selleks mitmesuguseid teabeallikaid. 4. Lahendab kasutajate turvaprobleemid kooskõlas veaparandusprotseduuridega. Vajadusel suunab probleemi lahendamiseks edasi. 5. Tõlgendab kasutaja turvaprobleeme süsteemselt, leiab neile lahendused. Kasutab vajalikke töövahendeid (kaugtoe tööriistu, seiresüsteeme) ning arvestab võimalikke kõrvaltoimeid. 6. Probleemi lahendamisel peab silmas lõpptulemust ja kliendi rahulolu.	
B.2.8 Muudatuste tugi (e-CF C2)	**EKR tase 5**
Tegevusnäitajad 1. Analüüsib ja hindab talitluslike/tehniliste muudatuste mõju süsteemile. 2. Rakendab muudatusi konkreetsetes IT-lahendustes, lähtudes juhistest, heast tavast, oma kogemustest ning infoturbe alastest protseduuridest. 3. Koostab tarkvara- või riistvaramuudatuste käikuandmise ajakava, riske käsitledes arvestab infosüsteemi otstarvet ning käideldavusnõudeid. 4. Minimeerib muudatustest tingitud teenusekatkestusi, järgib määratletud teenusetasemelepet, lähtub äriprotsesside katkematu toimimise vajadusest. 5. Kasutab IT-lahenduste haldusvahendeid koostöös IT-lahenduste korrashoiu ja arendamise eest vastutavate meeskondadega. 6. Osaleb teabevahetuses infosüsteemide lahenduste korrashoiu ja arendamise eest vastutavate IT-meeskondadega.	
B.2.9 Teenuse andmine (e-CF C3)	**EKR tase 5**
Tegevusnäitajad 1. Oma pädevuse piires tagab IT-teenuse stabiilse, turvalise ning tõhusa toimimise vastavalt kokkulepitud teenusetasemele. 2. Hindab ennetus- ja turvameetmeid, rakendab neid; infoturbe- ja jõudlusnõuete täidetuse seireks kasutab seiresüsteeme. 3. Seirab süsteemide talitluslikke näitajaid, tuvastab turvaintsidendid ja teenuste tõrked.	

4. Ajakohastab seire- ja haldustööriistu (nt skriptid, protseduurid), testib nende asjakohast tööd perioodiliselt. 5. Ajakohastab teenusega seotud dokumendid, registreerib kõik olulised sündmused ja intsidendid. 6. Teadaolevate infoturvariskide valguses analüüsib esmast teavet teenusetaset mõjutavatest sündmustest ning teavitab huvitatud osapooli. 7. Teeb ettepanekuid teenuse töökindluse parandamiseks ja turvataseme tõstmiseks. 8. Viib protsesse ellu kooskõlas organisatsiooni IKT teenuse strateegiaga.

B.2.10 Intsidendi- ja probleemihaldus (e-CF C4)	**EKR tase 5**
Tegevusnäitajad: 1. Registreerib infoturbejuhtumid töövoohaldussüsteemi vahenditega, märgistab need etteantud tunnuste järgi ning intsidendi kriitilisuse põhjal. 2. Tuvastab soovimatud kõrvalekalded infosüsteemi normaalsest tööst. 3. Tagab tõendite rikkumatuse, võimaldades turvaintsidendi edasist uurimist (nt õiguskaitseorganite, CERT, sisekontrolli poolt). 4. Vajadusel teavitab töötajaid ja partnereid juba toimunud või võimaliku intsidendi mõjust ning teeb juhtkonnale kerksusettepanekuid. 5. Tuvastab turvaintsidendi algpõhjused ja lahendab intsidendi lähtudes organisatsiooni protseduuridest. 6. Intsidendi mõju hindamisel arvestab infosüsteemi elementide ja süsteemi taristu omavahelisi seoseid ning toimet äriprotsessidele. 7. Suunab korduva intsidendi probleemihaldusse. 8. Osaleb IT ja infoturbehaldussüsteemi auditites ning on kaasatud riskihaldustoimingutesse.	

B.2.11 Infoturbestrateegia väljatöötamises osalemine (e-CF D1)	**EKR tase 5**
Tegevusnäitajad 1. Osaleb infoturbestrateegia väljatöötamises, lähtudes enamlevinud standarditest ja infoturbe heast tavast. 2. Osaleb olemasoleva olukorra kaardistamises ja annab soovitusi asjakohaste turvanõuete täitmiseks.	

B.2.12 Personaliarendus (e-CF D9)	**EKR tase 5**
Tegevusnäitajad 1. Annab sisendi infoturbealase koolitusvajaduse kaardistamisse. 2. Annab soovitused koolituste läbiviimiseks sobivate teenustajate osas. 3. Juhendab üksikisikuid ja meeskondi turvanõuete võimalike rikkumiste ennetamiseks ning nõustab neid intsidentide järgselt.	

B.2.13 Riskihaldus (e-CF E3)	**EKR tase 5**
Tegevusnäitajad 1. Kaardistab keskkonnapõhised infoturvariskid (veeb, võrk, pilv, mobiilsed seadmed jne). 2. Annab sisendi riskiregistri koostamisse ja riskiohjeplaanide haldusse, lähtudes heast tavast ja levinud raamistikest. 3. Viib ellu riskide leevendamiseks ja vältimiseks vajalikke tegevusi, arvestades koostatud plaane.	

B.2.14 Infoturbe haldamine (e-CF E8)	**EKR tase 5**
Tegevusnäitajad 1. Osaleb infoturbehalduses vastavalt oma pädevusele, sh intsidendihaldus, osalemine auditites. 2. Osaleb infovarade ja nende nõrkuste kaardistamisel, väiksemas organisatsioonis koordineerib neid tegevusi. 3. Annab sisendit infovaradele turvaklasside määramisel ning infovarade nõuetekohaseks käsitlemiseks. 4. Osaleb infoturvameetmete rakendusplaani koostamisel, lähtudes infoturbepoliitikast. 5. Määratleb andmete, varukoopiate, teenuseühenduste krüpteerimisvajaduse, lähtudes ärilistest vajadustest ja organisatsioonile kehtestatud nõuetest. 6. Koostöös IT-meeskonnaga koostab, haldab ja testib IT-süsteemide varundus- ja taasteplaane, lähtudes heast tavast ja tunnustatud raamistikest.	

KUTSET LÄBIVAD KOMPETENTSID

B.2.15 IT-turvaspetsialisti kutset läbiv kompetents	**EKR tase 5**
Tegevusnäitajad: 1. lähtub oma töös eetilistest tõekspidamistest;	

2. arvestab isiklike kutsealaste eesmärkide seadmisel organisatsiooni huve, kasutab organisatsiooni ressursse vastutustundlikult ja heaperemehelikult; 3. hindab kriitiliselt infoallikaid; 4. järgib elukestva õppe põhimõtet; 5. järgib tööprotsessi ohutusnõudeid; 6. järgib oma töös kehtestatud kvaliteedi ja infoturbe tagamise eeskirju; 7. kasutab dokumentide koostamisel ja suhtlemisel korrektset terminoloogiat; 8. suhtleb klientide ja kaastöötajatega, lähtudes heast tavast; 9. järgib valdkonnaga seotud õigusakte; 10. valdab eesti keelt tasemel B2, vene või inglise keelt tasemel B1 (vt Lisa 1).
Hindamismeetod(id): Läbivaid kompetentse hinnatakse teiste kutsestandardis toodud kompetentside hindamise käigus.

C-osa
ÜLDTEAVE JA LISAD

C.1 Teave kutsestandardi koostamise ja kinnitamise kohta ning viide ametite klassifikaatorile	
1. Kutsestandardi tähis kutseregistris	08-13112018-1.1/1k
2. Kutsestandardi koostajad	Peeter Hendrikson, Silberauto Eesti AS Toomas Lepik, Tallinna Tehnikaülikool Triin Muulmann, Kehtna Kutsehariduskeskus Raido Orumets, Baltic Computer Systems AS Rain Ottis, Tallinna Tehnikaülikool Heiki Tähis, Atea AS
3. Kutsestandardi kinnitaja	Infotehnoloogia ja Telekommunikatsiooni Kutsenõukogu
4. Kutsenõukogu otsuse number	12
5. Kutsenõukogu otsuse kuupäev	13.11.2018
6. Kutsestandard kehtib kuni	01.11.2023
7. Kutsestandardi versiooni number	1
8. Viide Ametite Klassifikaatorile (ISCO 08)	2529 Andmebaasi ja arvutivõrgu tippspetsialistid, mujal liigitamata
9. Viide Euroopa kvalifikatsiooniraamistikule (EQF)	5
C.2 Kutsenimetus võõrkeeles	
Inglise keeles	ICT Security Specialist, EstQF Level 5
C.3 Lisad	
Lisa 1 Keelte oskustasemete kirjeldused	