

E-ITSi põhineküpsusmudeli küsimustik (pilootversioon 2021-3)

Küsimustiku täitja (nimi): .....

Küsimustiku täitja roll:...

Täitmise kuupäev:....

Asutus:.....

Asutuse tegutsemise domeen: ...

Asutuse arvuti töökohtade arv:....

Asutuse geograafiliste lokatsioonide arv, mis sõltuvad ITKst: ....

Domeeni tähised	Domeenid	<p><b>Eesmärk:</b> pakkuda E-ITSi põhist asutustele infoturbealduse toimivuse mõõtmiseks korratavat ja võrreldavat tulemust nii isehindamiseks kui järelevalveks rakendamise erinevates elutsükli etappides.</p> <p><b>Juhis:</b> Märki allpool olevad punkteeritud väited,</p> <ul style="list-style-type: none"> <li>• mis hetkel kirjeldavad sinu organisatsiooni olukorda - rohelisega,</li> <li>• mis pigem on väitega koosõlas, kuid mõningate puudustega,</li> <li>• mis on osaliselt vastavuses olukorra kirjeldusele, kuid siiski oluliste puudustega, ja</li> <li>• mis võiks olla eesmärgiks, aga veel pole selleni jõudnud – punasega.</li> </ul> <p>• Valgeks jäta väited, mis ei käi sinu organisatsiooni kohta.</p>			
		<p><i>1. aste</i></p> <p>Toimetulek riskidega välise osapoolte abiga. Iga intsident võib põhjustada päevi kestva katkestuse, toimuda võivad suuremad andmelekked nii et riskiomanik seda ei tea või saab teada vaid välise osapoolte vahendusel. Andmevahetus võib põhjustada olulisi riske andmevahetuspartnerile.</p>	<p><i>2. aste</i></p> <p>Teostatud on infoturbe formaalsed nõuded, kuid organisatsiooni liikmed pole neist teadlikud ja neid ei pruugita jälgida. Toimuvatest intsidentidest pole inimesed teadlikud või ei tea kuidas nende korral käituda. Riskidega toimetulek on juhuslik ja väga suures sõltuvuses konkreetsest seotud inimesest. Infoturbe jätkusuutlikkus pole tagatud. Suur risk on ka andmevahetuspartneril.</p>	<p><i>3. aste</i></p> <p>Rakendatud on hädavajalik turvameetmete komplekt teadaolevate ohtudega toimetulekuks ja seotud riskide haldamiseks. Tagatud pole infoturbe jätkusuutlikkus samuti on ebakindel senitundmatute ohtude puhul reageerimine. Inimeste vahetumisel organisatsioonis on oht kiiresti langeda 2. astmele. Andmevahetus partneri jaoks on esmased riskid hallatud.</p>	<p><i>4.aste</i></p> <p>Asutus on valmis toime tulema ka täiesti uute riskidega. Inimesed teavad oma rolle ja vajalikke tegevusi avariiolekordas. Avariiolekordi on testitud ja taastamist katsetatud. Võimalikud katkestused äriprotsesside toimimist ja teenuseid oluliselt ei häiri. Intsidentide haldamisel kaasatakse välise osapoolte kompetentsi pigem vaid ulatuslike intsidentide korral. Andmevahetuspartnerite jaoks on tagatud kindlustunne ja usaldus.</p>
		<p><i>ALUSTAJA:</i> Head praktikaid pole rakendatud, riske pole teadvustatud, juhtkond pole initsiatiivi võtnud. Turvetegevused on juhuslikud ja pigem algatatud rohujuure tasandil.</p>	<p><i>DEFINEERITUD:</i> Protsessid ja tegevused on alustatud, kui toimuvad ad hoc. Dokumendid on koostatud, kuid osaliselt vananenud või ei vasta tegelikkusele.</p>	<p><i>PÕHITURVE:</i> Praktikad toimivad, on dokumenteeritud, ressursid plaanitud, rollid ja kohustused jaotatud. Tegevuste regulaarsus pole veel saavutatud.</p>	<p><i>STANDARDTURVE:</i> On selged üle organisatsioonilised poliitika ja printsiibid. Tegevusi seiratakse ja need on jälgitavad, tegevused on standardiseeritud ja dokumenteeritud. Toimub pidev parendamine. Erandeid seiratakse.</p>

<p><b>ISMS</b></p>	<p><b>Turbealdus</b></p> <p><i>Igas organisatsioonis sõltumata suurusest ja koosseisust</i></p>	<p>1. Infoturbe meetmed ja dokumentatsioon on uuendatud viimase 3 a jooksul.</p> <p>2. Infoturbealduse vajadus on teadvustatud ja kindlate eesmärkidega</p>	<p>3. Infoturbe haldus on algatatud juhtkonna tasemel.</p> <p>4. Kaardistatud on teenuste pakkumiseks kriitilised äriprotsessid ja nendega seotud varad ning vajalik kaitsetarve.</p> <p>5. On olemas esmane turvapoliitika.</p> <p>6. Jaotatud on infoturbe rollid ja kohustused.</p> <p>7. Infoturbe konfidentsiaaluse, tervikluse ja käideldavuse tarve on defineeritud kõigi äriprotsesside jaoks.</p>	<p>8. Infoturbe haldus elluviimiseks on eraldatud ressursid.</p> <p>9. Infoturbe rakendusplaan on töös, rakendatud on põhimeetmed.</p> <p>10. Infoturbe on integreeritud kõigisse protsessidesse, protsesside juhid jälgivad meetmete rakendatust oma protsessis.</p>	<p>11. Infoturbe halduse printsiibid on kõigile teada, neid uuendatakse regulaarselt (kord aastas).</p> <p>12. Toimuvad regulaarsed juhtkondlikud infoturbe läbivaatused (protokollid on säilitatud).</p>
<p><b>ORP</b></p>	<p><b>Organisatsioon ja personal</b></p> <p><i>Igas organisatsioonis sõltumata suurusest ja koosseisust</i></p>	<p>13. On koostatud kasutaja reeglid.</p> <p>14. Toimuvad sissejuhatavad koolitused</p> <p>15. Pääsuhalduses välditakse ad hoc lahendusi.</p>	<p>16. Jaotatud on infoturbe rollid ja määratletud kohustused.</p> <p>17. Lisaks sissejuhatavatele koolitustele on ka muid infoturbega seonduvaid koolitusi.</p> <p>18. Kasutaja reeglid on asja- ja ajakohased (sisekord, arvutikasutaja eeskiri).</p> <p>19. Protsesside juhid teavad oma protsessi ja teenustega seotud nõudeid ja kaitsetarvet.</p> <p>20. Asendamise jaoks on korraldatud reeglid (sh e-kirjavahetus, juurdepääsude haldus).</p>	<p>21. Juhtkond teab, mis olukord valitseb infoturbe korralduses ja mis on asutuse infoturbe nõuded.</p> <p>22. Protsesside juhid teavad oma protsessi nõrkusi ja riske ja haldavad neid kooskõlas organisatsiooni praktikate ja juhistega.</p> <p>23. Töötajad on reeglitest teadlikud ja järgivad neid.</p> <p>24. Asendamistel on selged reeglid ja need võimaldavad tööd jätkata.</p> <p>25. Pääsuhalduseks on kindlad reeglid, neid järgitakse ja seiratakse.</p>	<p>26. Personalipoliitika käsitleb kogu töötaja elutsükli haldust.</p> <p>27. Töökorraldust seiratakse ja parendatakse, toimub pidev teavitus.</p> <p>28. Organisatsioonis on toimiv toetav infoturbekultuur.</p> <p>29. Infoturbe koolitused on integreeritud ka muude koolituste ja teavitusürituste sisse.</p>
<p><b>CON</b></p>	<p><b>Kontseptsioonid ja meetodikad</b></p> <p><i>Igas organisatsioonis sõltumata suurusest ja koosseisust</i></p>	<p>30. On teadvustatud vajadus tegevuste IT standardiseerimiseks.</p>	<p>31. Krüptovahendite valimisel ja kasutamisel jälgitakse eeldefineeritud reegleid.</p> <p>32. Tarkvara ja rakenduste kasutuselevõtu eel teostatakse eelkontrolle. On loodud töökohtade riist ja tarkvarade profiilid.</p> <p>33. Läbi on viidud isikuandmete töötlemisemõjuhindangud ja määratletud vajalikud meetmed. Koostatud on privaatsuspoliitika.</p> <p>34. On koostatud andmevarunduse põhimõtted ja toimub andmete varundamine.</p>	<p>35. Mistahes tarkvaralise lahenduse hankimiseks, valimiseks ja kasutuselevõtuks on selged reeglid, mida järgitakse kogu tarkvara elutsükli arvesse võttes.</p> <p>36. On loodud töökohtade profiilid ja need võtavad arvesse äriprotsesside riske ja kaitsetarvet.</p> <p>37. Andmevarundust testitakse regulaarselt.</p> <p>38. Kasutajad on teadlikud andmevarunduse võimalustest ja piirangutest.</p>	<p>39. Kontseptsioonide, poliitikate, strateegiate asjakohasust seiratakse ja neid uuendatakse regulaarselt vastavalt organisatsiooni vajadustele ja uuenevatele nõuetele (regulaarsust tõendab läbivaatuste dokumenteerimine).</p>

<p><b>OPS</b></p>	<p><b>Käidutööd</b></p> <p><i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.</i></p>	<p>40. Haldustööde teostamiseks on pädev personal.</p> <p>41. Midagi logitakse.</p> <p>42. Rakendatud on kahjurprogrammide vastased tõrjeprogrammid.</p>	<p>43. Muudatuste halduseks on kokku lepitud protsess ja see on sobitatud äriprotsessidega.</p> <p>Uuendusvajadusi jälgitakse ja uuendused kontrollitakse ning rakendatakse.</p> <p>44. Enne tarkvara töösse lubamist seda testitakse hea tava kohaselt töökeskkonnast eraldi.</p> <p>45. Kaugtöö jaoks on reeglid ja kokkulepped, kuidas kaugtöö puhul töövahendeid hooldatakse.</p> <p>46. Väljast tellitavate teenuste jaoks on reeglid kokku lepitud.</p>	<p>47. IT-haldustööd on dokumenteeritud ja jälgitavad.</p> <p>48. Haldustööde teostamiseks on kokkulepitud teenustingimused.</p> <p>49. Toimub logide regulaarne läbivaatus, mille eeldusena on logide kogumine eesmärgistatud ja logide kellad on sünkroniseeritud.</p> <p>50. Väljast tellitavate teenuste osas on olemas avariiplaan ja selge teenustaseme lepe, mis sisaldab nii käideldavus-, terviklus- kui konfidentsiaalsusklausleid.</p>	<p>51. Muudatuste haldust seiratakse ja hinnatakse selle tulemuslikkust ja toimivust.</p> <p>52. On tsentraalne lubamatu juurdepääsu eest kaitstud logitaristu, milles andmeid analüüsitakse ja ebakõlade puhul alarmeeritakse.</p> <p>53. Kaughoolduse tõrke jaoks on koostatud ja testitud avariiplaan, mida vaadatakse regulaarselt läbi ja uuendatakse.</p> <p>54. Väljast tellitavaid teenuseid seiratakse ja hinnatakse regulaarselt. Muudatuste vajadusel teenuseid täpsustatakse ja arvestatakse alternatiivsete võimalustega.</p>
<p><b>DER</b></p>	<p><b>Avastamine ja reageerimine</b></p> <p><i>Intsidendihaldus ja auditid/läbivaatused</i></p> <p><i>Igas organisatsioonis sõltumata suurusest ja koosseisust</i></p>	<p>55. Kui turvaintsidendist teavitatakse, siis sellele reageeritakse jälgides kokkulepitud reegleid.</p> <p>56. On teadvustatud infoturbe auditi kohustus.</p>	<p>57. Turvasündmustest teavitamiseks on loodud kanal ja kõik turvasündmused registreeritakse turvasündmuste registris.</p> <p>58. On loodud esmameetmete juhend turvaintsidenti puhuks.</p> <p>59. Infoturbe auditi läbimiseks valmistatakse ette eelkõige formaalsed dokumendid.</p> <p>60. Kokku on lepitud avarii korral inimeste rollid ja kommunikatsiooni kanalid.</p>	<p>61. On määratletud, millised on kriitilised võrgusegmendid, mida jälgitakse.</p> <p>62. Välisallikaid jälgitakse teabe analüüsiks ja riskide hindamiseks (raportid).</p> <p>63. Turvasündmuste asitõendeid säilitatakse.</p> <p>64. Ulatuslikemate turvasündmuse jaoks on loodud eskaleerimise strateegia ja kommunikatsiooni protseduur.</p> <p>65. Infoturbe auditi tulemusi analüüsitakse ja need on lisatud infoturbe rakendusplaani.</p> <p>66. On loodud avariikontseptsioon, millesse on kaasatud kõik äriprotsessid, seda on töötajatele tutvustatud.</p>	<p>67. Toimub regulaarne avastussüsteemide läbivaatus ja realiseeritud on võimalusel ka automaatalarmid.</p> <p>68. Kasutaja ja IT haldurid osalevad regulaarselt infoturbe õppustel.</p> <p>69. Toimuvad regulaarsed infoturbe sise- ja välisauditid, mis on aluseks juhtkondlikele läbivaatustele ja infoturbe edasise eelarve plaanimisele.</p> <p>70. Regulaarselt toimuvad avariiohupused ja rakendatakse <i>Red Teamingut (lõkktestimine)</i>.</p>
<p><b>APP</b></p>	<p><b>Rakendused</b></p> <p><i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.</i></p> <p><i>Kliendirakendused, Kataloogiteenused, võrguteenused, ärirakendused, rühmatarkvara</i></p>	<p>71. Rakenduste kasutuselevõtul jälgitakse rakendustele antavaid õigusi ja neid piiratakse.</p> <p>72. Toimub rakenduste ja andmebaaside konfiguratsioonide haldus</p> <p>73. Rühmatarkvara on kasutusele võetud</p>	<p>74. Kasutajad saavad hoiatusteavitusi võimalike kasutaja rakenduste ohtude eest.</p> <p>75. Kataloogiteenustele (directory service) on kehtestatud reeglid ja üldine turvapoliitika.</p> <p>76. On defineeritud lubatud rakendused.</p> <p>77. Asutuse siseseks kasutamiseks määratletud andmete veebirakendustes töötlemiseks on vajalik autentimine.</p> <p>78. Organisatsiooni domeeninimedega halduse eest vastutab konkreetne inimene.</p>	<p>79. Kasutuses on arvutite keskhaldus</p> <p>80. Bürootarkvara hooldust korraldab selleks koolitunud rollitaitja.</p> <p>81. Kataloogiteenused (directory service, nt AD, LDAP) haldab vaid vastav haldur.</p> <p>82. Kataloogiteenustele (directory service) on rakendatud rühmapoliitikad.</p> <p>83. Iga kasutajakontot on võimalik seostada konkreetse töötajaga.</p> <p>84. Halduskontode paroolid on turvalised ja kordumatud.</p> <p>85. Serverid ja klientarvutid salvestavad paroole vaid räsikujul.</p> <p>86. Pääsuõiguste dokumentatsioon vastab tegelikule seisule.</p> <p>87. Veebirakenduste lähtekood on kaitstud lubamatu juurdepääsu eest.</p>	<p>94. Rakenduste tarbeks on loodud nõuete nimekirjad. Enne kasutusele võttu rakenduse ühilduvuse tagamiseks seda testitakse.</p> <p>95. Dokumentide saatmisel muutmise kaitseks need digiallkirjastatakse.</p> <p>96. Veebibrausereid konfigureeritakse keskselt.</p> <p>97. Kataloogiteenuse (directory service) tegevusi seiratakse ja logitakse, logiandmeid vaadatakse regulaarselt läbi. Logid säilitatakse 1.a.</p> <p>98. Veebiserveri turvalisust kontrollitakse läbistustestidega regulaarselt (nt iga auditi käigus).</p> <p>99. Sama domeeninime kasutamisel on domeeni nimeruum selgelt jaotatud avalikuks ja organisatsioonisiseseks osaks.</p>

				<p>88. Välistes võrkudes kasutatakse andmeside kaitseks krüpteeritud sideprotokolle (TLS-i ja protokolle HTTPS).</p> <p>89. Organisatsiooni domeeninimed on regulaarselt ja aegsasti pikendatud.</p> <p>90. Andmebaasi turvasündmusi logitakse koos ajatempliga, logid on muutmis- ja ülekirjutuskaitstud.</p> <p>91. Andmebaasid on varundatud.</p> <p>92. Rühmatarkvara klient on kasutaja jaoks eelkonfigureeritud.</p> <p>93. Serveri vaikekontode nimetused ja paroolid on muudetud, tarbetud vaikekontod on desaktiveeritud.</p>	<p>100. Andmebaaside varunduse taastet ja terviklust testitakse ja kontrollitakse regulaarselt.</p> <p>101. On rakendatud meilimanuste automaatse avamise piirangud.</p>
<b>SYS</b>	<p><b>IT-süsteemid</b></p> <p><i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.</i></p> <p><i>Server, arvuti, mobiilseadmed, muud seadmed</i></p>	<p>102. Serveritele on juurdepääs vaid pääsuõigusega isikutel.</p> <p>103. Serverites on kasutusel kahjurtõrje tarkvara.</p> <p>104. Printerid ja kontorikombainid on paigutatud asukohtadesse, kus töötamine seadmega on teistele töötajatele märgatav ja kus ei käi ilma saatjata külalisi.</p> <p>105. Printeri või kontorikombaini läheduses asub paberipurusti või hävitamisele minevate paberdokumentide konteiner.</p>	<p>106. Serveri tarkvara, teenuste ja kontode konfiguratsioon on dokumenteeritud.</p> <p>107. On dokumenteeritud, milliseid tegevusi serverites logitakse ja mis tingimustel logisid vaadatakse.</p> <p>108. Klientarvutit on võimalik kasutada ainult end nõuetekohaselt autentitud kasutajal.</p> <p>109. Klientarvutil on vähemalt kaks kasutajakontot: haldusõigustega konto ja tavakasutaja konto.</p> <p>110. Klientarvutites on otsustatud, milliseid pilvteenuseid ja millises ulatuses on lubatud kasutada.</p> <p>111. Organisatsioonis on kehtestatud kord sülearvuti kaotamisest, vargusest või rikkest teavitamiseks.</p> <p>112. Organisatsioonis on koostatud ja kehtestatud mobiiltelefonide kasutamise eeskiri.</p> <p>113. Serverite süsteemifailidele juurdepääsu õigus on ainult süsteemihalduritel.</p>	<p>114. Serveri kasutusevõtu eel on koostatud serveri kasutuse kava, milles on defineeritud rakendamise otstarve, riistvaranõuded, integreerimine teiste rakendustega (nt kataloogi teenustega) ja varundamise korraldus)</p> <p>115. Varundussüsteemid on varundatavatest serveritest füüsiliselt eraldatud ja asuvad eri tuletõkkeseksioonides.</p> <p>116. Kasutaja autendib serverisse ainult isikustatud kasutajakontoga.</p> <p>117. Enne paikade ja uuendite serverisse installimist on nende turvalisust, ühilduvust ja toimet testitud testserveril.</p> <p>118. On tõendatavalt testitud, et varundatud andmeid on võimalik serveris taastada ja neid on pärast taastamist võimalik ettenähtud viisil kasutada.</p> <p>119. Serverite kahjurtõrje tarkvara on uuendatud regulaarselt.</p> <p>120. Logisid analüüsitakse regulaarselt.</p> <p>121. Virtualiseerimissüsteemi rakendamise eeldused on täidetud ja kontrollitud (virtuaaltaristu host-serveril on virtualiseerimissüsteemi jaoks piisavad andmesideühendused; virtualiseerimissüsteemis kasutatavate rakenduste eraldamise ja kapseldamise nõuded on täidetud; virtualiseerimissüsteem vastab käideldavuse ja andmeedastusjõudluse nõuetele).</p>	<p>131. Server on ühendatud piisava võimsuse ja aku kestvusega puhvertoiteallikaga (UPS), mille aku kestvus on kontrollitud regulaarselt.</p> <p>132. Serverisse on installitud ainult serveri otstarbe täitmiseks vajalikud teenused.</p> <p>133. Regulaarsed serveri turbetestimised on dokumenteeritud.</p> <p>134. Teenuseid väljapoole organisatsiooni andvad serverid on paigutatud demilitaartsooni (<i>demilitarized zone</i>, DMZ).</p> <p>135. Kõik serverite konfiguratsioonimuudatused ja turvalisust puudutavad toimingud on dokumentatsiooni (nt automaatne logi) alusel jälgitavad.</p> <p>136. Serverite taastekava (ingl <i>disaster recovery plan</i>) rakendamist harjutatakse regulaarselt.</p> <p>137. Seirevahendid teavitavad ettenähtud piirnäitajate ületamisest ja tõrgete tekkimisest koheselt käituspersonali.</p> <p>138. Kasutajad omavad üksnes selliseid õigusi ja neil on juurdepääs üksnes sellistele funktsioonidele, teenustele ja andmetele, mida nad vajavad oma tööülesannete täitmiseks (teadmistarbe põhimõte).</p> <p>139. Klientarvuti mikrofone ja kaamerat ei kasutata ilma kasutaja nõusolekuta. Klientarvutiga ühendatakse vaid lubatud seadmeid. Seadmete lubamine on dokumenteeritud.</p> <p>140. Klientarvutid on lülitatud kesksesse seiresüsteemi.</p>

				<p>122. Haldusõigusega kasutajakontot klientarvutites kasutatakse ainult klientarvuti halduseks. Haldusõigusega konto alt ei tehta tavatoiminguid.</p> <p>123. Regulaarselt varundatakse klientarvutitest vähemalt need andmed, mida ei saa muudest andmetest tuletada.</p> <p>124. Klientarvutitesse paigaldatud keskselt hallatav kahjurvaratõrje tarkvara.</p> <p>125. Kasutajale on antud kirjutusõigused ainult konkreetset määratud failisüsteemi piirkonnas. Kasutajatel ei ole kirjutusõigust operatsioonisüsteemi ja rakenduste kaustades.</p> <p>126. Sülearvutis on aktiveeritud personaalne tulemüür.</p> <p>127. Seadmenimed ei anna teavet kasutaja isiku kohta ega sisalda organisatsioonile viitavaid elemente (nt mobiiltelefonid).</p> <p>128. Printerite ja kontorikombainide konfigureerimine juhtpaneeli ja veebiserveri kaudu on paroolikaitsega. Parool on teada ainult volitatud kasutajatel.</p> <p>129. Esemevõrgu (IoT) seadmete pääs sisevõrku on võimalikult kitsendatud. Seadmed ise on kaitstud lubamatu füüsilise juurdepääsu eest.</p> <p>130. Töötajad teavad, milliseid andmeid on lubatud irdandmekandjatele salvestada ja mis tingimustel on lubatud irdandmekandjaid organisatsioonist välja viia.</p>	<p>141. Klientarvutite jaoks on loodud etaloninstall. Installimise käigus kloonitakse sobivalt eelkonfigureeritud etaloninstall klientarvutisse. Etaloninstall sisaldab kõiki konfiguratsioonimuudatusi, uuendeid ja turvapaiku ning on eelnevalt testitud ja testimised dokumenteeritud.</p> <p>142. Klientarvutite digitaalsed assistendid on desaktiveeritud.</p> <p>143. Sülearvutite kettad on krüpteeritud.</p> <p>144. Klientarvutis allalaetavaid faile ei avata automaatselt.</p> <p>145. Arvutisse sisselogimisel on kasutusel mitmikautentimine (nt 2FA).</p> <p>146. Organisatsiooni sisevõrku sisselogimine on võimalik ainult selleks lubatud sülearvutitel (nt sertifikaadipõhise seadmete autentimise abil).</p> <p>147. Kasutaja ei saa iseseisvalt muuta veebirakenduste ja meiliklientide turvaseadeid.</p> <p>148. Pääs sülearvutist sisevõrku toimub krüpteeritud, virtuaalse privaatsvõrgu (VPN) kaudu.</p> <p>149. Nutitelefonid või tahvelarvuti SIM-kaart on kaitstud vaikeseadistusest erineva PIN-koodiga.</p> <p>150. Vajaduse puudumisel või kasutamise vaheaegadel on mobiiltelefonide raadioliidesed (nt WLAN või Bluetooth) desaktiveeritud.</p> <p>151. Kui esemevõrgu seadmed (nt valvekaamerad) kuuluvad mingisse laiemas otstarbega süsteemi (nt hoone halduse süsteemi), vahetavad nad andmeid ainult selle süsteemiga. Esemevõrgu seadme kuulumisel laiemasse IT-süsteemi on seadme otsepääs Internetti blokeeritud.</p>
<b>IND</b>	<b>Tööstus</b>  <i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.</i>	152. Tööstusautomaatika välise haldajaga on olemas teenusleping.	153. Tööstusautomaatika komponentide andmevahetuspartnerid ja andmekategooriad on dokumenteeritud. 154. Robotseadme tarnijaga on sõlmitud tugiteenusleping.	155. Käidutehnoloogiate algparoolid on asendatud. 156. Tööstusautomaatika on integreeritud turvapoliitika osaks. 157. On määratud ja dokumenteeritud, milliseid automaatikakomponentide andmeid ja sündmusi logitakse, kui kaua logiandmeid säilitatakse ja kes tohib logidele juurde pääseda.	161. Tööstusautomaatika kasutamisel on väljatöötatud tsoonikontseptsioon. Käidutehnoloogia taristu on dokumenteeritud. 162. Juurdepääs hooldusliidestele on piiratud selleks õigust omavate isikutega. 163. Tööstusautomaatika täielik dokumentatsioon on tõrgete korral kättesaadav. 164. Avalikes võrkudes edastatavad mõõte- ja juhtandmed on kaitstud turvaliste andmeside protokollidega.

	<i>Käidu-ja juhtimistehnika, tööstusautomaatika (sh SCADA, robotid, targad majad)</i>			<p>158. Käidutehnoloogia ja tööstusautomaatika komponentide tarbetud liidesed, teenused, funktsioonid on desaktiveeritud või desinstallitud.</p> <p>159. Tööstusautomaatika komponendid on lahutatud kontori IT-süsteemidest, komponentide suhtlus teiste komponentidega on vajaduspõhine ja võimalikult minimaalne.</p> <p>160. Robotseadme kaughoolduse tegemisel ei pääse hoolduse tegija juurde organisatsiooni muudele süsteemidele või robotseadmetele.</p>	<p>165. Andureid kalibreeritakse regulaarselt, kalibreerimine dokumenteeritakse.</p> <p>166. Ohutusautomaatika seadmeid hallatakse vastavalt õigusnormidele ja ohutusstandarditele.</p> <p>167. Ohutusautomaatika muutujate väärtusepiirid on määratletud ja piirini jõudmisest alarmeeritakse.</p>
<b>NET</b>	<p><b>Võrgud ja side</b></p> <p><i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.</i></p> <p><i>Võrgud, võrgukomponendid, side</i></p>	<p>168. Arvutivõrgu haldusega on seotud kindel rollitaitja.</p> <p>169. Võrgutopoloogia on dokumenteeritud.</p>	<p>170. Võrgutopoloogia põhimõtted on dokumenteeritud ja uuendatud vähemalt viimase 3 a jooksul.</p> <p>171. Võrguseadmete haldamiseks ja käitamiseks on dokumenteeritud reeglid.</p> <p>172. Raadiokohtvõrgu kasutamise eeskirjas on fikseeritud, milliste sisemiste ja väliste võrkudega tohib raadiokohtvõrgu klienti ühendada.</p>	<p>173. Võrk on dokumenteeritud ja uuendused lisatakse koheselt (on ajakohane).</p> <p>174. Võrk on segmenteeritud kooskõlas kaitsetarbe eripärasega.</p> <p>175. Kõigi võrgukomponentide vaikeparoolid on vahetatud.</p> <p>176. Võrguseadmete tootja poolt väljastatud turvauuendid (ingl <i>security update</i>) ja turbepaigad (ingl <i>security patch</i>) paigaldatakse peale avaldamist võimalikult kiiresti.</p> <p>177. Võrguhalduslahendused on varundatud (seadistused, logid, sündmusteated).</p> <p>178. Kasutatakse ajakohast krüptomehhanismi traadita side turvamiseks (nt WPA3). Lihtsalt murtavate krüpteerimisprotokollide (nt WEP, WPA) kasutamine on blokeeritud</p> <p>179. Kõigis võrguhalduse komponentides ja nendega seotud võrgukomponentides on aeg sünkroniseeritud ning kasutatakse sama ajavööndit.</p> <p>180. Telefoni keskjaama vaikeparoolid on asendatud piisavalt tugevate paroolidega.</p>	<p>181. Regulaarse võrguhalduse ülevaatuse käigus kontrollitakse võrguhalduse dokumentatsiooni ajakohasust, vastavust hetkeseisule ning tegelikele protseduuridele (&gt;1 ülevaatuse protokoll).</p> <p>182. Võrgukomponentide ja võrguhaldusvahenditega seotud olulistest sündmustest teavitatakse automaatselt kohe pärast sündmuse toimumist vastutavat IT-personali.</p> <p>183. Võrguhaldusvahendite ja võrgukomponentide konfiguratsioonid on varundatud ja on osa organisatsiooni taasteplaanist.</p> <p>184. Raadiovõrgust kohtvõrgule juurdepääsu on lubatud ainult tulemüüri kaudu.</p> <p>185. Tulemüüre seiratakse, logid säilitatakse ja määratletud sündmuste puhul toimub automaatteavitus.</p>
<b>INF</b>	<p><b>Taristu</b></p> <p><i>Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema</i></p>	<p>186. Hooned vastavad tuleohutusnõuetele ja rakendatud on sissehoidmise vastaseid meetmeid.</p>	<p>187. Ruumiplaneeringus on arvesse võetud turvaliste tsoonide olemasolu ja rajatud selle tarbeks eraldi pääsusüsteemid ja põhimõtted (nt uste lukustamine). Arvesse on võetud kaitstavate ruumide erivajadusi (torustike puudumine, gaaskustutus vms serveriruumides).</p> <p>188. Toimib külaliste järelevalve.</p>	<p>190. Toimib pääsu ja võtmehaldus, reeglid on dokumenteeritud ja teadvustatud.</p> <p>191. Kasutuseeta kaablid on kasutusest kõrvaldatud.</p> <p>192. Töökoha dokumente säilitatakse vastavalt kokkulepitud reeglitele.</p> <p>193. Kaabelduste ja torustike plaanid on kehtivad.</p> <p>194. Kaabeldused on arusaadavalt tähistatud ja dokumenteeritud.</p>	<p>195. On toimunud regulaarsed ja praktilised tuleohutusõppused.</p> <p>196. Serveriruumi mõõdikuid ja seadmeid seiratakse ja testitakse regulaarselt, tulemused on dokumenteeritud, vajadusel seadmeid uuendatakse.</p> <p>197. Võrgu dokumentatsiooni ajakohastatakse muudatuste põhised ja vaadatakse läbi regulaarselt.</p>

	<i>jälitatavad SLA vormis.</i>  <i>Hooned, ruumid, kaabeldus</i>		189. On rajatud nõuetekohane serveriruum, mille pääs on piiratud asjakohaste rollidega.		
--	--	--	---	--	--