E-ITSi esmarakendajate isehindamise küpsusmudeli küsimustik (pilootversioon 2021-1)

Küsimustiku täitja: .....
Täitmise kuupäev:....
Asutus:.....

Domeeni tähised	Domeenid				
		Eesmärk: pakkuda E-ITSi põhist asutustele infoturbehalduse toimivuse mõõtmiseks korratavat ja võrreldavat tulemust nii isehindamiseks kui järelevalveks rakendamise erinevates elutsükli etappides. **Juhis:** Märgi allpool olevad punkteeritud väited, • mis hetkel kirjeldavad sinu organisatsiooni olukorda - rohelisega, • mis osaliselt vastavad olukorra kirjeldusele– kollasega, ja • mis võiks olla eesmärgiks, aga veel pole selleni jõudnud – punasega. • Valgeks jäta väited, mis ei käi sinu organisatsiooni kohta.			
		1. aste *Toimetulek riskidega väliste osapoolte abiga. Iga intsident võib põhjustada päevi kestva katkestuse, toimuda võivad suuremad andmelekked nii et riskiomanik seda ei tea või saab teada vaid väliste osapoolte vahendusel. Andmevahetus võib põhjustada olulisi riske andmevahetuspartnerile.*	*2. aste* *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.*	*3. aste* *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.*	*4.aste* *Asutus on valmis toime tulema ka täiesti uute riskidega. Inimesed teavad oma rolle ja vajalikke tegevusi avariiolukorras. Avariiolukordi on testitud ja taastamist katsetatud. Võimalikud katkestused äriprotsesside toimimist ja teenuseid oluliselt ei häiri. Intsidentide haldamisel kaasatakse väliste osapoolte kompetentsi pigem vaid ulatuslike intsidentide korral. Andmevahetuspartnerite jaoks on tagatud kindlustunne ja usaldus.*
		ALUSTAJA: Head praktikaid pole rakendatud, riske pole teadvustatud, juhtkond pole initsiatiivi võtnud. Turvetegevused on juhuslikud ja pigem algatatud rohujuure tasandil.	*FORMAALNE: Protsessid ja tegevused on alustatud, kui toimuvad ad hoc. Dokumendid on koostatud, kuid osaliselt vananenud või ei vasta tegelikkusele.*	*PÕHITURVE: Praktikad toimivad, on dokumenteeritud, ressursid plaanitud, rollid ja kohustused jaotatud. Tegevuste regulaarsus pole veel saavutatud.*	*STANDARDTURVE: On selged üle organisatsioonilised poliitikad ja printsiibid. Tegevusi seiratakse ja need on jälgitavad, tegevused on standardiseeritud ja dokumenteeritud. Toimub pidev parendamine. Erandeid seiratakse.*
ISMS	**Turbehaldus** *Igas organisatsioonis*	• Infoturbe haldus on juhuslik ilma kindlate eesmärkideta, valdavalt dokumenteerimata v	• Infoturbe haldus on algatatud juhtkonna tasemel. Kaardistatud on teenuste pakkumiseks kriitilised	• Infoturbe haldus elluviimiseks on eraldatud ressursid. • Infoturbe rakendusplaan on töös, rakendatud on põhimeetmed.	• Infoturbe halduse printsiibid on kõigile teada, neid uuendatakse regulaarselt (kord aastas).

	sõltumata suurusest ja koosseisust	dokumentatsioon on vananenud (uuendamata viimase 3 a jooksul).	äriprotsessid ja nendega seotud varad ning vajalik kaitsetarve. • On olemas esmane turvapoliitika. • Jaotatud on infoturbe rollid ja kohustused. • Osad infoturbe teemad on deklaratiivsel tasemel, sest ressursid on puudulikud ja vajadus teadvustamata.	• Infoturve on integreeritud kõigisse protsessidesse, protsesside juhid jälgivad meetmete rakendatust oma protsessis.	• Toimuvad regulaarsed juhtkondlikud infoturbe läbivaatused (protokollid on säilitatud).
ORP	**Organisatsioon ja personal** *Igas organisatsioonis sõltumata suurusest ja koosseisust*	• Juhised ja eeskirjad on kohati vananenud ja on formaalsed • Toimuvad sissejuhatavad koolitused • Pääsuhaldus on korraldatud ad hoc.	• Jaotatud on infoturbe rollid ja määratletud kohustused. • Lisaks sissejuhatavatele koolitustele on ka muid infoturbega seonduvaid koolitusi. • Loodud on asja- ja ajakohased kasutaja reeglid (sisekord, arvutikasutaja eeskiri). • Protsesside juhid teavad oma protsessi ja teenustega seotud nõudeid ja kaitsetarvet.	• Juhtkond teab, mis olukord valitseb infoturbe korralduses ja mis on asutuse infoturbe nõuded. • Protsesside juhid teavad oma protsessi nõrkusi ja riske ja haldavad neid kooskõlas organisatsiooni praktikate ja juhistega. • Töötajad on reeglitest teadlikud ja järgivad neid. • Asendamistel on selged reeglid. • Pääsuhalduseks on kindlad reeglid, neid järgitakse ja seiratakse.	• Personalipoliitika käsitleb kogu töötaja elutsükli haldust. • Töökorraldust seiratakse ja parendatakse, toimub pidev teavitus. • Organisatsioonis on toimiv toetav infoturbekultuur. • Infoturbe koolitused on integreeritud ka kõigi muude koolituste ja teavitusürituste sisse.
CON	**Kontseptsioonid ja metoodikad** *Igas organisatsioonis sõltumata suurusest ja koosseisust*	• On teadvustatud vajadus tegevuste standardiseerimiseks, kuid selle realiseerimisega pole veel alustatud.	• Krüptovahendite valimisel ja kasutamisel jälgitakse eeldefineeritud reegleid. • Tarkvara ja rakenduste kasutuselevõtu eel teostatakse eelkontrolle. On loodud töökohtade riist ja tarkvarade profiilid. • Läbi on viidud isikuandmete töötlemisemõjuhinnangud ja määratletud vajalikud meetmed. Koostatud on privaatsuspoliitika. • On koostatud andmevarunduse põhimõtted ja toimub andmete varundamine.	• Mistahes tarkvaralise lahenduse hankimiseks, valimiseks ja kasutuselevõtuks on selged reeglid, mida järgitakse kogu tarkvara elutsüklit arvesse võttes. • On loodud töökohtade profiilid ja need võtavad arvesse äriprotsesside riske ja kaitsetarvet. • Andmevarundust testitakse regulaarselt. • Kasutajad on teadlikud andmevarunduse võimalustest ja piirangutest.	• Kontseptsioonide, poliitikate, strateegiate asjakohasust seiratakse ja neid uuendatakse regulaarselt vastavalt organisatsiooni vajadustele ja uuenevatele nõuetele (regulaarsus tõendab läbivaatuste dokumenteerimine).
OPS	**Käidutööd**	• Haldustööde teostamiseks on pädev personal.	• Muudatuste halduseks on kokku lepitud protsess ja see on sobitatud äriprotsessidega. Uuendusvajadusi jälgitakse ja	• IT-haldustööd on dokumenteeritud ja jälgitavad. • Haldustööde teostamiseks on kokkulepitud teenustingimused.	• Muudatuste haldust seiratakse ja hinnatakse selle tulemuslikkust ja toimivust.

	Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.	• Midagi logitakse, , aga puudub selge arusaam, mis logidega edasi tehakse. • Rakendatud on kahjurprogrammide vastased tõrjeprogrammid.	uuendused kontrollitakse ning rakendatakse. • Enne tarkvara töösse lubamist seda testitakse hea tava kohaselt töökeskkonnast eraldi. • Kaugtöö jaoks on reeglid ja kokkulepped, kuidas kaugtöö puhul töövahendeid hooldatakse. • Väljast tellitavate teenuste jaoks on reeglid kokku lepitud.	• Toimub logide regulaarne läbivaatus, logide kellad on sünkroniseeritud ja logide kogumine on eesmärgistatud. • Väljast tellitavate teenuste osas on olemas avariiplaan ja selge teenustaseme lepe, mis sisaldab nii käideldavus, terviklus kui konfidentsiaalsus klausleid.	• On tsentraalne lubamatu juurdepääsu eest kaitstud logitaristu, milles andmeid analüüsitakse ja ebakõlade puhul alarmeeritakse. • Kaughoolduse tõrke jaoks on koostatud ja testitud avariiplaan, mida vaadatakse regulaarselt läbi ja uuendatakse. • Väljast tellitavaid teenuseid seiratakse ja hinnatakse regulaarselt. Muudatuste vajadusel teenuseid täpsustatakse ja arvestatakse alternatiivsete võimalustega.
DER	**Avastamine ja reageerimine** *Intsidendihaldus ja auditid/läbivaatused* *Igas organisatsioonis sõltumata suurusest ja koosseisust*	• Kui turvaintsidendist teavitatakse, siis sellele reageeritakse. . Otseseid reegleid pole. • On teadvustatud infoturbe auditi kohustus.	• Turvasündmustest teavitamiseks on loodud kanal ja kõik turvasündmused registreeritakse turvasündmuste registris. • On loodud esmameetmete juhend turvaintsidendi puhuks. • Infoturbe auditi läbimiseks valmistatakse ette eelkõige formaalsed dokumendid. • Kokku on lepitud avarii korral inimeste rollid ja kommunikatsiooni kanalid.	• On määratletud, millised on kriitilised võrgusegmendid, mida jälgitakse. • Välisallikaid jälgitakse teabe analüüsiks ja riskide hindamiseks (raportid). • Turvasündmuste asitõendeid säilitatakse. • Ulatuslikemate turvasündmuse jaoks on loodud eskaleerimise strateegia ja kommunikatsiooni protseduur. • Infoturbe auditi tulemusi analüüsitakse ja need on lisatud infoturbe rakendusplaani. • On loodud avariikontseptsioon, millesse on kaasatud kõik äriprotsessid, seda on töötajatele tutvustatud.	• Toimub regulaarne avastussüsteemide läbivaatus ja realiseeritud on võimalusel ka automaatalarmid. • Kasutajad ja IT haldurid osalevad regulaarselt infoturbe õppustel. • Toimuvad regulaarsed infoturbe sise- ja välisauditid, mis on aluseks juhtkondlikele läbivaatustele ja infoturbe edasise eelarve plaanimisele. • Regulaarselt toimuvad avariiõppused ja rakendatakse *Red Teamingut.*
APP	**Rakendused** *Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.* *Kliendirakendused, Kataloogiteenused, võrguteenused, ärirakendused, rühmatarkvara*	• Rakenduste kasutuselevõtul jälgitakse rakendustele antavaid õigusi ja neid piiratakse. • Rakenduste ja andmebaaside konfiguratsioone hallatakse ilma selgete reegliteta. • Rühmatarkvara kasutuselevõtul konfigureerib oma kliendi igaüks ise.	• Kasutajad saavad hoiatusteavitusi võimalike kasutaja rakenduste ohtude eest. • Kataloogiteenustele on kehtestatud reeglid ja üldine turvapoliitika. • On defineeritud lubatud rakendused. • Veebirakenduste kasutamiseks on alati vajalik autentimine. • Organisatsiooni domeeninimede halduse eest vastutab konkreetne inimene. • Asendamise jaoks on korraldatud reeglid (sh e-kirjavahetus, juurdepääsude haldus).	• Kasutuses on arvutite keskhaldus v büroorakenduste hooldust korraldab selleks koolitunud rollitäitja. • Kataloogiteenuseid haldab vaid vastav haldur. • Kataloogiteenustele on rakendatud rühmapoliitikad. • Iga kasutajakontot on võimalik seostada konkreetse töötajaga. • Halduskontode paroolid on turvalised ja kordumatud. • Serverid ja klientarvutid salvestavad paroole vaid räsikujul. • Pääsuõiguste dokumentatsioon vastab tegelikule seisule. • Veebirakenduste lähtekood on kaitstud lubamatu juurdepääsu eest. • Välistes võrkudes kasutatakse andmeside kaitseks TLS-i ja protokolli HTTPS.	• Rakenduste tarbeks on loodud nõuete nimekirjad. Enne kasutusele võttu rakenduse ühilduvuse tagamiseks seda testitakse. • Dokumentide saatmisel muutmise kaitseks need digiallkirjastatakse. • Veebibrausereid konfigureeritakse keskselt. • Kataloogiteenuse tegevusi seiratakse ja logitakse, logiandmeid vaadatakse regulaarselt läbi. Logid säilitatakse 1.a. • Veebiserveri turvalisust kontrollitakse läbitustestidega regulaarselt (nt iga auditi käigus). • Sama domeeninime kasutamisel on domeeni nimeruum selgelt jaotatud avalikuks ja organisatsioonisiseseks osaks. • Andmebaaside varunduse taastet ja terviklust testitakse ja kontrollitakse regulaarselt. • On rakendatud meilimanuste automaatse avamise piirangud.

				• Organisatsiooni domeeninimed on regulaarselt ja aegsasti pikendatud. • Andmebaasi turvasündmusi logitakse koos ajatempliga, logid on muutmis- ja ülekirjutuskaitstud. • Andmebaasid on varundatud. • Rühmatarkvara klient on kasutaja jaoks eelkonfigureeritud. • Serveri vaikekontode nimetused ja paroolid on muudetud, tarbetud vaikekontod on desaktiveeritud.	
SYS	IT-süsteemid *Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.* *Server, arvuti, mobiilseadmed, muud seadmed*	• Serveritele on juurdepääs vaid pääsuõigusega isikutel. • Serverites on kasutusel kahjurtõrje tarkvara. • Printerid ja kontorikombainid on paigutatud asukohtadesse, kus töötamine seadmega on teistele töötajatele märgatav ja kus ei käi ilma saatjata külalisi. • Printeri või kontorikombaini läheduses asub paberipurusti või hävitamisele minevate paberdokumentide konteiner.	• Serveri tarkvara, teenuste ja kontode konfiguratsioon on dokumenteeritud. • On dokumenteeritud, milliseid tegevusi serverites logitakse ja mis tingimustel logisid vaadatakse. • Klientarvutit on võimalik kasutada ainult end nõuetekohaselt autentinud kasutajal. • Klientarvutil on vähemalt kaks kasutajakontot: haldusõigustega konto ja tavakasutaja konto. • Klientarvutites on otsustatud, milliseid pilvteenuseid ja millises ulatuses on lubatud kasutada. • Organisatsioonis on kehtestatud kord sülearvuti kaotamisest, vargusest või rikkest teavitamiseks. • Organisatsioonis on koostatud ja kehtestatud mobiiltelefonide kasutamise eeskiri. • Serverite süsteemifailidele juurdepääsu õigus on ainult süsteemihalduritel. • Kasutaja eemaloleku ja mitte kasutamise ajaks lukustab kasutaja oma seadmete	• Varundussüsteemid on varundatavatest serveritest füüsiliselt eraldatud ja asuvad eri tuletõkkesektsioonides. • Kasutaja autendib serverisse ainult isikustatud kasutajakontoga. • Enne paikade ja uuendite serverisse installimist on nende turvalisust, ühilduvust ja toimet testitud testserveril. • On tõendatavalt testitud, et varundatud andmeid on võimalik serveris taastada ja neid on pärast taastamist võimalik ettenähtud viisil kasutada. • Serverite kahjurtõrje tarkvara on uuendatud regulaarselt. • Logisid analüüsitakse regulaarselt. • Enne virtualiseerimissüsteemi rakendamist on kontrollitud, kas: virtuaaltaristu host-serveril on virtualiseerimissüsteemi jaoks piisavad andmesideühendused; virtualiseerimissüsteemis käitatavate rakenduste eraldamise ja kapseldamise nõuded on täidetud; virtualiseerimissüsteem vastab käideldavuse ja andmeedastusjõudluse nõuetele. • Haldusõigusega kasutajakontot klientarvutites kasutatakse ainult klientarvuti halduseks. Haldusõigusega konto alt ei tehta tavatoiminguid. • Regulaarselt varundatakse klientarvutitest vähemalt need andmed, mida ei saa muudest andmetest tuletada. • Klientarvutitesse paigaldatud keskselt hallatav kahjurvaratõrje tarkvara. • Kasutajale on antud kirjutusõigused ainult konkreetselt määratud failisüsteemi piirkonnas. Kasutajatel ei ole kirjutusõigust operatsioonisüsteemi ja rakenduste kaustades.	• Server on ühendatud piisava võimsuse ja aku kestvusega puhvertoiteallikaga (UPS), mille aku kestvust on kontrollitud regulaarselt. • Serverisse on installitud ainult serveri otstarbe täitmiseks vajalikud teenused. • Regulaarsed serveri turbetestimised on dokumenteeritud. • Teenuseid väljapoole organisatsiooni andvad serverid on paigutatud demilitaartsooni (*demilitarized zone*, DMZ). • Kõik serverite konfiguratsioonimuudatused ja turvalisust puudutavad toimingud on dokumentatsiooni (nt automaatne logi) alusel jälgitavad. • Serverite taastekava (ingl *disaster recovery plan*) rakendamist harjutatakse regulaarselt. • Seirevahendid teavitavad ettenähtud piirnäitajate ületamisest ja tõrgete tekkimisest koheselt käituspersonali. • Kasutajad omavad üksnes selliseid õigusi ja neil on juurdepääs üksnes sellistele funktsioonidele, teenustele ja andmetele, mida nad vajavad oma tööülesannete täitmiseks (teadmistarbe põhimõte). • Klientarvuti mikrofoni ja kaamerat ei kasutata ilma kasutaja nõusolekuta. Klientarvutiga ühendatakse vaid lubatud seadmeid. Seadmete lubamine on dokumenteeritud. • Klientarvutid on lülitatud kesksesse seiresüsteemi. • 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.

			(arvuti, telefon, tahvelarvuti) ekraanid.	• Sülearvutis on aktiveeritud personaalne tulemüür. • Seadmenimed ei anna teavet kasutaja isiku kohta ega sisalda organisatsioonile viitavaid elemente (mobiiltelefonid). • Printerite ja kontorikombainide konfigureerimine juhtpaneeli ja veebiserveri kaudu on paroolikaitsega. Parool on teada ainult volitatud kasutajatel. • Esemevõrgu (IoT) seadmete pääs sisevõrku on võimalikult kitsendatud. Seadmed ise on kaitstud lubamatu füüsilise juurdepääsu eest. • Töötajad teavad, milliseid andmeid on lubatud irdandmekandjatele salvestada ja mis tingimustel organisatsioonist välja viia.	• Klientarvutite digitaalsed assistendid on desaktiveeritud. • Sülearvutite kettad on krüpteeritud. • Klientarvutis allalaetavaid faile ei avata automaatselt. • Arvutisse sisselogimisel on kasutusel mitmikautentimine (nt 2FA). • Organisatsiooni sisevõrku sisselogimine on võimalik ainult selleks lubatud sülearvutitel (nt sertifikaadipõhise seadmete autentimise abil). • Kasutaja ei saa iseseisvalt muuta veebirakenduste ja meiliklientide turvaseadeid. • Pääs sülearvutist sisevõrku toimub krüpteeritult, virtuaalse privaatvõrgu (VPN) kaudu. • Nutitelefoni või tahvelarvuti SIM-kaart on kaitstud vaikeseadistusest erineva PIN-koodiga. • Vajaduse puudumisel või kasutamise vaheaegadel on mobiiltelefonide raadioliidesed (nt WLAN või Bluetooth) desaktiveeritud. • Kui esemevõrgu seadmed (nt valvekaamerad) kuuluvad mingisse laiema otstarbega süsteemi (nt hoone halduse süsteemi), vahetavad nad andmeid ainult selle süsteemiga. Esemevõrgu seadme kuulumisel laiemasse IT-süsteemi on seadme otsepääs Internetti blokeeritud.
IND	**Tööstus** *Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.* *Käidu-ja juhtimistehnika, tööstusautomaatika (sh SCADA, robotid, targad majad)*	• Tööstusautomaatikat haldab vajaduspõhiselt väline lepinguta osapool.	• Käidutehnoloogiate algparoolid on asendatud. • Tööstusautomaatika komponentide andmevahetuspartnerid ja andmekategooriad on dokumenteeritud. • Robotseadme tarnijaga on sõlmitud tugiteenuseleping.	• Tööstusautomaatika on integreeritud turvapoliitika osaks. • On määratud ja dokumenteeritud, milliseid automaatikakomponentide andmeid ja sündmusi logitakse, kui kaua logiandmeid säilitatakse ja kes tohib logidele juurde pääseda. • Käidutehnoloogia ja tööstusautomaatika komponentide tarbetud liidesed, teenused, funktsioonid on desaktiveeritud või deinstallitud. • Tööstusautomaatika komponendid on lahutatud kontori IT-süsteemidest, komponentide suhtlus teiste komponentidega on vajaduspõhine ja võimalikult minimaalne. • Robotseadme kaughoolduse tegemisel ei pääse hoolduse tegija juurde organisatsiooni muudele süsteemidele või robotseadmetele.	• Tööstusautomaatika kasutamisel on väljatöötatud tsoonikontseptsioon. Käidutehnoloogia taristu on dokumenteeritud. • Juurdepääs hooldusliidestele on piiratud selleks õigust omavate isikutega. • Tööstusautomaatika täielik dokumentatsioon on tõrgete korral kättesaadav. • Avalikes võrkudes edastatavad mõõte- ja juhtandmed on kaitstud turvaliste andmeside protokollidega. • Andureid kalibreeritakse regulaarselt, kalibreerimine dokumenteeritakse. • Ohutusautomaatika seadmeid hallatakse vastavalt õigusnormidele ja ohutusstandarditele. • Ohutusautomaatika muutujate väärtusepiirid on määratletud ja piirini jõudmisest alarmeeritakse.
NET	**Võrgud ja side**	• Asutuse võrk on üles seatud juhuslikult. Selget vastutajat	• Võrgutopoloogia on põhimõtteliselt dokumenteeritud, kuid kõik	• Võrk on dokumenteeritud ja uuendused lisatakse koheselt (on ajakohane).	• Regulaarse võrguhalduse ülevaatuse käigus kontrollitakse võrguhalduse dokumentatsiooni

	Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis. *Võrgud, võrgukomponendid, side*	võrguhalduse eest rollina pole. Võrgu dokumentatsioon ei vasta tegelikkusele või puudub.	uuendused pole dokumenteeritud. • Võrguseadmete haldamiseks ja käitamiseks on dokumenteeritud reeglid. • Raadiokohtvõrgu kasutamise eeskirjas on fikseeritud, milliste sisemiste ja väliste võrkudega tohib raadiokohtvõrgu klienti ühendada.	• Võrk on segmenteeritud kooskõlas kaitsetarbe eripärasega. • Kõigi võrgukomponentide vaikeparoolid on vahetatud. • Võrguseadmete tootja poolt väljastatud turvauuendid (ingl *security update*) ja turbepaigad (ingl *security patch*) paigaldatakse peale avaldamist võimalikult kiiresti. • Võrguhalduslahendused on varundatud (seadistused, logid, sündmusteated). • Kasutatakse IEEE 802.11i-2004 (krüptomehhanism WPA2) või uuemat standardit (WPA3) . WEP ja WPA kasutamine on blokeeritud. • Kõigis võrguhalduse komponentides ja nendega seotud võrgukomponentides on aeg sünkroniseeritud ning kasutatakse sama ajavööndit. • Vaikeparoolid on enne telefonikeskjaama kasutuselevõttu asendatud piisavalt tugevate paroolidega.	ajakohasust, vastavust hetkeseisule ning tegelikele protseduuridele (>1 ülevaatuse protokolli). • Võrgukomponentide ja võrguhaldusvahenditega seotud olulistest sündmustest teavitatakse automaatselt kohe pärast sündmuse toimumist vastutavat IT-personali. • Võrguhaldusvahendite ja võrgukomponentide konfiguratsioonid on varundatud ja on osa organisatsiooni taasteplaanist. • Raadiovõrgust kohtvõrgule juurdepääsu on lubatud ainult tulemüüri kaudu. • Tulemüüre seiratakse, logid säilitatakse ja määratletud sündmuste puhul toimub automaatteavitus.
INF	Taristu *Kui käidutöödeks kasutatakse väliseid teenuseid, siis vastavad nõuded peaks olema jälitatavad SLA vormis.* *Hooned, ruumid, kaabeldus*	• Hooned vastavad tuleohutusnõuetele ja rakendatud on sissemurdmise vastaseid meetmeid.	• 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). • Toimib külaliste järelevalve. • On rajatud nõuetekohane serveriruum, mille pääs on piiratud asjakohaste rollidega.	• Toimib pääsu ja võtmehaldus, reeglid on dokumenteeritud ja teadvustatud. • Kasutuseta kaablid on kasutusest kõrvaldatud. • Töökoha dokumente säilitatakse vastavalt kokkulepitud reeglitele. • Kaabelduste ja torustike plaanid on kehtivad. • Kaabeldused on arusaadavalt tähistatud ja dokumenteeritud.	• Regulaarsed tuleohutusõppused. • Serveriruumi mõõdikuid ja seadmeid seiratakse ja testitakse regulaarselt, tulemused on dokumenteeritud, vajadusel seadmeid uuendatakse. • Võrgu dokumentatsiooni ajakohastatakse muudatuste põhiselt ja vaadatakse läbi regulaarselt.