ALGTEKST-TERVIKTEKST

Kinnitatud kantsleri 10.09.2025 korraldusega nr 175

Redaktsiooni jõustumise kuupäev: 10.09.2025

**Serverite- ja võrguhalduse põhimõtted**

1. **Üldine**
   1. Serverite ja võrguhalduse eesmärk on kirjeldada põhimõtted võrgu ja serverite haldamisel.
   2. Käesolev dokument sätestab Tallinna Tehnikaülikooli (edaspidi Ülikool) võrguhalduse ja serverite haldamise põhimõtted ning nõuded, lähtudes ISO/IEC 27001 standardist. Dokument määratleb vajalikud kontrollmeetmed, vastutusvaldkonnad ja protseduurid, et tagada ülikooli infotehnoloogia taristu (edaspidi IT taristu) turvalisus ja järjepidevus.
2. **Serverihaldus**
   1. Ülikooli serverihaldus peab tagama IT taristu töökindluse, turvalisuse ja kättesaadavuse, lähtudes ISO/IEC 27001 standarditest. Serverihalduse eesmärk on luua stabiilne, turvaline ja optimeeritud serverikeskkond, mis toetab ülikooli akadeemilisi, teadus- ja haldustegevusi ning kaitseb turvaohtude ja rikkumiste eest. Serverihaldus hõlmab nii füüsiliste kui ka virtualiseeritud serverite haldust.
   2. **Serverite arendamine, kavandamine ja arhitektuur**
      1. Serverikeskkonna arendamisel, kavandamisel ja haldamisel lähtutakse turvalisusest, töökindlusest ja tulevikuvajadustest. Tegevused peavad toetama ülikooli strateegilisi eesmärke ning akadeemilisi ja haldusprotsesse, tagades stabiilse ja turvalise infrastruktuuri.
      2. Arendusprotsess peab tagama süsteemide jätkusuutlikkuse, kavandamine toetab tõhusat haldust ning haldamine peab kindlustama töökindluse ja turvataseme. Uuendused ja laiendused viiakse ellu parimate praktikate ja ajakohaste tehnoloogiate alusel, minimeerides katkestuste mõju. Selleks kasutatakse proaktiivset planeerimist ja hooldusaknaid, mis võimaldavad sujuvat üleminekut uutele lahendustele.
      3. Töökindluse suurendamiseks rakendatakse koormuse tasakaalustamist ja kõrgkäideldavust, et vältida ülekoormust ja ühe tõrkepunkti riske. Enne uuenduste juurutamist tuleb lahendused testida ja valideerida, et tagada olemasoleva IT-arhitektuuriga ühildumine.
      4. Serverite arhitektuur peab vastama ülikooli IT- ja infoturbepoliitikatele ning toetama tsoonipõhist turvalisust ja võrgusegmentatsiooni. Serverid jaotatakse funktsionaalseteks gruppideks, arvestades nii töökindluse kui ka turvalisuse nõudeid. Teenuste eraldatus võib toimuda nii füüsilisel kui ka virtualiseerimise tasandil.
      5. Arhitektuur tuleb kujundada nii, et erinevate turvatsoonide vahel tagada piisav loogiline ja füüsiline eraldatus, vältimaks haavatavuste levikut ühest süsteemist teise.
   3. **Füüsilise serveri kasutuselevõtt ja hankimine**
      1. Füüsilise serveri kasutuselevõtt ja hankimine peab toimuma läbimõeldult ning vastavuses ülikooli tehniliste, funktsionaalsete ja turvanõuetega. Kavandamisel tuleb hinnata serveri riistvara, operatsioonisüsteemi ja rakendustarkvara sobivust, et tagada jõudlus, töökindlus ning ühildumine olemasoleva IT-infrastruktuuriga.
      2. Tehnilised parameetrid, sealhulgas sooritusvõime, mälumaht, läbilaskevõime ja sideliideste tüüp, peavad vastama eeldatavale kasutuskoormusele. Lisaks tuleb arvesse võtta serverite ruumivajadust, konstruktsioonitüüpi, serverikappide paigutust, energiatarvet ja soojuseraldust, et tagada pikaajaline töökindlus ja vältida ülekuumenemist.
      3. Haldusliideste kaitse peab olema tagatud, piirates juurdepääsu administratiivsetele funktsioonidele ning kasutades turvalisi haldusprotokolle *(nt SSH, HTTPS)*.
      4. Serverite hankimine toimub läbipaistva ja dokumenteeritud protsessi kaudu, mis hõlmab nõuete spetsifikatsiooni koostamist, toodete võrdlust ning sobivuse hindamist füüsiliste mõõtmete ja tehniliste parameetrite alusel. Hankimisel tuleb hinnata serveri funktsionaalsust ja integreeritavust olemasolevatesse süsteemidesse ning pöörata tähelepanu töökindlusele ja haldusmugavusele, tuginedes usaldusväärsetele infoallikatele ja tootjadokumentatsioonile.
      5. Lisaks arvestatakse kogu elutsükli kulusid, sealhulgas soetus- ja püsikulusid, ning tootjapoolseid tugiteenuseid ja hoolduslepinguid, mis võimaldavad kiiret reageerimist tõrgete korral. Hankimise ja paigaldamise käik dokumenteeritakse, et tagada süsteemide jälgitavus ja haldusprotsessi läbipaistvus.
   4. **Füüsiliste serverite töökindlus, turvalisus ja toitepüsivus**
      1. Ülikooli kesksete füüsiliste serverite töökindluse, turvalisuse ja teenuste järjepidevuse eest vastutab ülikooli IT-osakond. Ülikoolis võivad esineda ka üksuste hallatavad serverid, mille töökindluse ja turvalisuse tagamine on vastava üksuse vastutusel. Kõik serverid peavad vastama samadele nõuetele, mis on sätestatud käesolevas dokumendis. Üksustel on võimalus vajadusel paigutada oma serverid ülikooli IT-osakonna hallatavasse serveriruumi või kujundada oma serveriruumid vastavaks nõuetele. Serverid tuleb paigaldada turvalistesse ruumidesse, kus on piiratud ligipääs ja rakendatud kaheastmeline autentimine (nt ligipääsukaart koos PIN-koodiga). Füüsiline juurdepääs peab olema kontrollitud ligipääsukaartide, võtmete või biomeetriliste lahenduste abil, et tagada ligipääs üksnes volitatud isikutele.
      2. Serveriruumides tuleb rakendada sobivaid seire- ja turvasüsteeme (nt kaamerad, liikumisandurid), mis võimaldavad kiiret ohu tuvastamist ja reageerimist. Juurdepääsude logimine peab hõlmama sisenemiste ja väljumiste registreerimist ning juurdepääsuõiguste regulaarset ülevaatamist ja ajakohastamist.
      3. Serverite töökindluse ja toitekatkestuste taluvuse tagamiseks peavad seadmed olema ühendatud sobiva võimsuse ja aku kestvusega puhvertoiteallikaga (edaspidi UPS). UPS peab tagama stabiilsuse lühiajaliste katkestuste korral ja võimaldama sujuvat üleminekut varutoitele või kontrollitud süsteemi sulgemist. Vajaduse korral tuleb kasutada täiendavat generaatorit või muud pikaajalist varutoitelahendust.
      4. UPS-i kasutamisel tuleb tagada järgmised tingimused:
         1. piisav võimsus kriitiliste serverite ja võrguseadmete töö tagamiseks kuni varutoiteallika aktiveerumiseni;
         2. regulaarne hooldus ja testimine, mis kinnitab töökindlust ja akude vastavust;
         3. seirevõimekus, mis võimaldab varajast hoiatust aku tühjenemise või tõrgete korral;
         4. dokumenteerimine, mis kajastab konfiguratsiooni, hooldusgraafikut ja intsidendilogi (*sh Confluence’is*).
      5. Operatsioonisüsteemid ja tarkvara tuleb hankida usaldusväärsetest allikatest. Serverid tuleb konfigureerida vastavalt turvalise algseadistuse põhimõtetele – eemaldada mittevajalikud teenused ja ligipääsud ning vähendada ründepind miinimumini. Käivitusprotsess peab olema turvaline, kasutades *UEFI Secure Boot’i* ning eemaldades mittevajalikud võtmed.
      6. Juurdepääsuõigused määratletakse selgelt ja püsivara ning alglaadimise seadeid tohivad muuta üksnes volitatud isikud. Ajasünkroniseerimine toimub organisatsiooni ajastandardi alusel, tagades logide täpsuse ja võrreldavuse. Serverite seadistused ja muudatused dokumenteeritakse, et tagada läbipaistvus ja halduse järjepidevus.
   5. **Virtuaalserverite haldamine, turvalisus ja juurdepääsukontroll**
      1. Ülikooli kesksete virtuaalserverite, hüperviisorite ja virtualiseeritud keskkondade halduse eest vastutab ülikooli IT-osakond, kes tagab süsteemide töökindluse, turvalisuse ja järjepidevuse. Ülikoolis võivad virtuaalservereid hallata ka üksused ise, kuid nende hallatavad keskkonnad peavad vastama käesolevas dokumendis sätestatud nõuetele. IT-osakond annab vajadusel nõu, kuidas nõudeid täita, kuid vastutus virtuaalserverite halduse eest jääb servereid haldavale üksusele.
      2. Kõik virtuaalserverite kasutus- ja juurdepääsutoimingud peavad olema kontrollitud ja logitud, et ennetada volitamata ligipääsu ning toetada turvaintsidentide uurimist.
      3. Haldus peab toimuma turvalises virtualiseerimiskeskkonnas, mis on konfigureeritud vastavalt tootja turvajuhistele. Hüperviisorid, virtuaalmasinad ja konteinerid seadistatakse füüsilise ja loogilise eraldatuse tagamiseks, vältimaks turvariske ja andmeleket.
      4. Lähtuda tuleb turvalise algseadistuse põhimõtetest: eemaldada mittevajalikud teenused ja ligipääsud ning minimeerida ründepinda. Halduse juures tuleb rakendada tugevat autentimist ja rollipõhist õiguste jaotust. Juurdepääsud, õiguste muudatused ja autentimised logitakse ning vaadatakse regulaarselt üle.
      5. Juurdepääsukontroll peab põhinema kasutaja rollil ja tööülesannetel ning vastama infotehnoloogiliste varade halduse korrale. Autentimiseks kasutatakse keskseid lahendusi ja isikustatud kasutajakontosid, et tagada tegevuste auditeerimine ja identiteedi jälgitavus. Kui ligipääs eeldab kõrgemat turvataset, rakendatakse kaheastmelist autentimist (MFA).
      6. Serveri haldusõigused määratakse minimaalse vajalikkuse põhimõttel – tavatoiminguteks kasutatakse piiratud kontot ning administratiivseid tegevusi teostatakse kõrgendatud õigustega kontoga.
      7. Ajasünkroniseerimine peab olema kooskõlas organisatsiooni ajastandardiga, et tagada logide täpsus. Turvaseaded vaadatakse regulaarselt üle, eriti enne uute serverite käivitamist või pärast muudatusi.
   6. **Serverites andmete krüpteerimine**
      1. Serverites andmete krüpteerimise vajadus määratakse infoturbealase riskihinnangu alusel. Kui riskihinnang näitab krüpteerimisvajadust, tuleb tundlikud failid ja andmekandjad kaitsta vastavalt ülikooli infoturbenõuetele, kasutades usaldusväärseid vahendeid ning järgides krüptokontseptsiooni põhimõtteid.
      2. Ligipääs krüpteeritud andmetele peab toimuma rollipõhise kontrolli kaudu, tagades juurdepääsu ainult neile, kelle tööülesanded seda eeldavad. Krüpteerimine rakendatakse andmekandjatele – sealhulgas kõvaketastele, SSD-dele, välistele salvestusseadmetele ja virtuaalmasinaid sisaldavatele andmemassiividele – juhul kui need sisaldavad tundlikku või konfidentsiaalset teavet.
      3. Krüpteerimis- ja taasteparoolide haldus peab toimuma turvalises keskkonnas, näiteks sertifitseeritud paroolihoidlas, mis välistab loata juurdepääsu ning võimaldab süsteemi taastamist vajaduse korral. Krüpteerimise, ligipääsuhalduse ja andmekaitse seadistuste muudatused tuleb dokumenteerida, et tagada läbipaistvus ja kontrollitavus.
   7. **Serverite monitooring, kahjurvaratõrje ja anomaaliate tuvastamine**
      1. Füüsilised ja virtuaalserverid peavad olema pideva seire ja logimise all, et tuvastada turvaohtusid, süsteemirikkeid, kõrvalekaldeid ja ebatavalist tegevust. Teenuseid ja protsesse jälgitakse spetsialiseeritud seirevahenditega, mis võimaldavad reaalajas olukorra hindamist ja varajast reageerimist intsidentidele.
      2. Kahjurvaratõrje rakenduste kasutamine peab olema põhjendatud ning vastama infoturbenõuetele. Tõrjetarkvara vajadus määratakse serveri operatsioonisüsteemi, teenuste ja olemasolevate turvamehhanismide põhjal, vältides liigset ressursikasutust ja jõudlusprobleeme. Kasutatav lahendus peab võimaldama tuvastada kahjurvara ka pakitud andmete puhul *(compressed data scanning)*. Seadistused ja uuendused dokumenteeritakse tagamaks läbipaistvus ja jälgitavus.
      3. Logimine peab vastama ülikooli logimise poliitikale. Analüüsitakse regulaarselt juurdepääsu- ja kasutusmustreid, et tuvastada võimalikke turvarikkumisi või süsteemi väärkasutust. Logitavate sündmuste hulka kuuluvad süsteemi käivitused ja taaskäivitused, sisselogimised ja nende katsed, utiliitide kasutus, õiguste ületamised, tulemüürireeglite rikkumiskatsed, kontomuudatused, turvatõrked ja hoiatusteated.
      4. Seire peab hõlmama vähemalt järgmisi valdkondi:
         1. jõudlus- ja tervisenäitajad: protsessorikasutus, mälumaht, kettakasutus, võrguliiklus ja töötavad protsessid. Süsteem peab võimaldama kriitiliste kõrvalekallete automaatset tuvastamist ja teavitust.
         2. tulemüüride ja turvalahenduste seisund: IDS/IPS, viirusetõrje ning nende uuenduste ja aktiivsuse jälgimine. Kõrvalekallete korral tuleb anda kohene hoiatus.
         3. failisüsteemi ja konfiguratsioonide terviklikkuse kontroll: tundlikke faile ja süsteemikonfiguratsioone tuleb kontrollida tervikluse tagamise tööriistadega (*integrity tools*), et avastada volitamata muudatusi.
         4. teenuste saadavus: ärikriitilised teenused (nt andmebaasid, veebiserverid, autentimisteenused) peavad olema pideva kättesaadavuse kontrolli all. Tõrgete ilmnemisel teavitatakse vastutavaid osapooli.
         5. keelatud ja kõrvalekalduvate protsesside seire: protsesside jälgimine põhineb lubatud rakenduste nimekirjal. Kahtlaste protsesside ilmnemisel edastatakse automaatne teavitus.
         6. anomaaliate ja käitumispõhine seire: kasutatakse mehhanisme, mis tuvastavad kõrvalekaldeid tavapärasest süsteemi- või kasutajakäitumisest, sealhulgas võimalusel tehisintellektil põhinevaid lahendusi.
         7. monitooringuandmete kaitse ja säilitamine: andmed peavad olema kaitstud volitamata juurdepääsu, muutmise ja kustutamise eest ning säilitatud samade nõuete alusel nagu logid. Vajaduse korral arhiveeritakse.
         8. seiresüsteemide testimine ja audit: monitooringumeetmete toimivust testitakse regulaarselt (nt simulatsioonide või katkestuskatsete abil). Tulemused dokumenteeritakse ja vajadusel rakendatakse parandusmeetmeid.
      5. Serverite turvaintsidente käsitletakse vastavalt kehtestatud korrale „Pöördumiste, intsidentide, sündmuste ja probleemide haldus“. Seadistused, vastutused ja toimimisjuhised peavad olema dokumenteeritud ja ajakohased. Seire- ja logimismeetmete tõhusust hinnatakse regulaarselt, arvestades tuvastatud riske, uusi ohte ja tehnoloogia arengut.
   8. **Serveritel paiknevate infosüsteemide ja muude infotehnoloogiste varade haldus**
      1. Ülikooli serveritel paiknevad infosüsteemide, rakenduste ja muude infotehnoloogiliste varade, mis toetavad organisatsiooni protsesse ja teenuseid, haldus peab toimuma süsteemselt ja järjepidevalt, et tagada töökindlus, turvalisus ja vastavus kehtestatud nõuetele.
      2. Haldustegevuste aluseks on keskne register, kuhu on kantud olulised infosüsteemid ja tehnoloogilised varad. Iga süsteem ja varaline objekt määratakse vastutavale omanikule, kelle ülesanne on tagada haldus, administreerimine ja vastavus ülikooli infoturbenõuetele.
      3. Süsteemihaldurid, partnerid või kolmandad osapooled viivad läbi igapäevaseid haldustoiminguid ja tehnilisi muudatusi vastavalt kehtestatud reeglitele. Nende vastutusalasse kuulub:
         1. IT-arenduskeskkondade haldus – arendus-, test- ja tootmiskeskkondade toimimine ning tööprotsesside tagamine;
         2. seadistuste ja tehniliste muudatuste teostamine – süsteemide ja rakenduste konfigureerimine, vajalike uuenduste läbiviimine;
         3. infoturbenõuete täitmine – autentimise, juurdepääsukontrolli ja krüptomeetmete rakendamine;
         4. ligipääsude regulaarne ülevaatus ja ajakohastamine – nt võrguligipääsud ja lokaalsed kontod, mille puhul eemaldatakse õigused, mida enam ei vajata;
         5. tehniline dokumentatsioon ja taastetõendamine – süsteemikirjeldused, taastejuhendid ja varundustestid;
         6. varundamine ja andmekaitse – andmete varundamine kooskõlas poliitikatega ja taastamisjuhistega;
         7. monitooringu seadistamine ja testimine – süsteemide jälgimine vastavalt projektijuhi tellimusele ja toimimise regulaarne testimine;
         8. muudatuste haldus – rakendustes, süsteemides ja serverites tehtud muudatuste dokumenteerimine vastavalt protseduuridele;
         9. intsidendi- ja probleemihalduse tugi – osalemine intsidentide ja probleemide lahendamisel, sealhulgas veaallikate tuvastamine;
         10. tehniliste riskide hindamine ja parendusettepanekud – süsteemide ja seadmete seisukorra hindamine ning parenduste soovitamine;
         11. logifailide analüüs ja koormuse hindamine – logide kontroll ning süsteemide jõudluse ja koormuse analüüs.
      4. Süsteemihaldurid tegutsevad õiguslike aluste ja konfidentsiaalsusnõuete kohaselt. Ilma selge põhjenduseta ega volituseta ei tohi vaadata logisid, andmeid ega teisi ressursse, mis ei ole otseselt seotud tööülesannetega. Tegevused peavad olema jälgitavad ja vastama ülikooli andmekaitsepoliitikale, infoturbenõuetele ja isikuandmete kaitse seadustele. Juurdepääs tundlikele andmetele ja logidele peab olema põhjendatud ja auditeeritav.
      5. Süsteemihaldurite tegevused kuuluvad regulaarse auditi ja järelevalve alla, et tuvastada volitamata tegevusi ja potentsiaalseid turvariske. Rikkumiste või nõuete eiramise korral rakendatakse asjakohaseid sanktsioone, sealhulgas hoiatusi, juurdepääsu piiramist, töösuhte lõpetamist või muid meetmeid.
      6. Iga süsteemihaldur vastutab enda hallatavate süsteemide töökindluse, turvalisuse ja nõuetele vastavuse eest, tagades, et ülikooli infosüsteemid ja varad toimivad katkestusteta, turvaliselt ja tõhusalt, kooskõlas kehtivate protseduuride ja poliitikatega.
   9. **Virtuaalserverite ja infosüsteemide regulaarne turbetestimine**
      1. Virtuaalserverite ja infosüsteemide turvalisuse tagamiseks tuleb regulaarselt hinnata rakendatud tehniliste turvameetmete tõhusust ja vastavust kehtestatud infoturbepõhimõtetele. Turbetestimine hõlmab süsteemide tehnilise seisundi analüüsi, eesmärgiga tuvastada puudujääke ligipääsukontrollis, konfiguratsioonides ja süsteemikäitumises.
      2. Testimisel hinnatakse vähemalt järgmisi aspekte:
         1. ligipääsukontrollide toimimine ja õiguste sobivus, sh ebavajalike või liigsete privileegide olemasolu;
         2. autentimismehhanismide vastavus turvanõuetele, sealhulgas paroolipoliitika kehtivus ja vajadusel mitmeastmelise autentimise rakendamine;
         3. süsteemide ja teenuste konfiguratsioonide turvalisus, lähtudes parimatest praktikatest ja turvastandarditest.
      3. Turbetestide ulatus ja sagedus määratakse riskihindamise põhjal, tagades, et testimine ei häiri süsteemide tööd. Testimise käigus kogutud andmeid käsitletakse konfidentsiaalselt ning need tehakse kättesaadavaks ainult volitatud isikutele.
      4. Testide tulemused dokumenteeritakse ning vajaduse korral algatatakse parandustegevused vastavalt tuvastatud puudustele.
   10. **Serverite, infosüsteemide ja infotehnoloogiliste varade turvapaikade haldus**
       1. Serverite, infosüsteemide ja muude IT-varade turvapaikade ning süsteemiuuenduste rakendamine peab toimuma järjepidevalt, et kõrvaldada kriitilised ja kõrge riskitasemega haavatavused kehtestatud ajaraamis. Kriitiliste süsteemide puhul tuleb minimeerida teenusekatkestusi, planeerides paigaldused hooldusakende ajal.
       2. Süsteemihaldurid vastutavad hallatavate süsteemide turvauuenduste jälgimise, planeerimise ja rakendamise eest, tuginedes usaldusväärsetele teabeallikatele. Nad peavad olema kursis tehnoloogiliste arengutega ning reageerima turvaohtudele kiiresti ja asjakohaselt. Tõsistest haavatavustest ja riskidest tuleb viivitamatult teavitada infoturbejuhti.
       3. Turvapaikade ja süsteemiuuenduste rakendamisega seotud tegevused dokumenteeritakse vastavalt ülikooli turvanõrkuste haldamise korrale. Paikade rakendamine ja uuenduste järjepidevus kuuluvad süsteemihalduri vastutusalasse.
   11. **Serverite ja infosüsteemide varundamine ning taastehaldus**
       1. Serverite ja infosüsteemide varundamine ning taastehaldus toimub vastavalt ülikooli talitluspidevuse poliitikale. Käesolev punkt sätestab varundusstrateegia ja põhimõtted, mille alusel tagatakse andmete säilimine ning süsteemide operatiivne taastamine rikete või intsidentide korral.
       2. Varundusprotsess peab hõlmama:
          1. kriitiliste andmete regulaarset varundamist vastavalt määratletud ajakavale;
          2. varukoopiate turvalist salvestamist, tervikluse kontrolli ja juurdepääsu piiramist;
          3. varundus- ja taastamisprotseduuride dokumenteerimist, läbivaatust ja testimist.
       3. Infotehnoloogiliste varade omanikud vastutavad selle eest, et andmete klassifikatsioon ja säilitamispoliitika oleksid kooskõlas varundusnõuetega ning et vajalikud andmekogumid oleksid hõlmatud varundamisega.
       4. Serverid ja infosüsteemid tuleb varundada regulaarselt, tuginedes andmekaitsevajadusele ja infosüsteemi kaardil määratletud nõuetele.
       5. Varukoopiad tuleb hoida turvalises, füüsiliselt ja elektrooniliselt kaitstud asukohas, eelistatult geograafiliselt hajutatult. Kohapealseid varundusandmeid säilitatakse keskkonnas, kus on piiratud juurdepääs ning kaitse tule- ja veekahjustuste vastu. Varundatud andmed tuleb krüpteerida vastavalt valdkonna standarditele. Juurdepääs varundustele toimub vähima privileegi põhimõttel.
       6. Tervikluse tagamiseks kasutatakse kontrollsummasid (nt CRC, hash-väärtused) või muid räsipõhiseid meetodeid (nt SHA-256, digitaalne sõrmejälg). Süsteemihaldurid peavad tagama, et nende hallatavad süsteemid vastavad varundusnõuetele ning taastamine on tehniliselt toimiv ja tõrgeteta. Selleks kontrollitakse regulaarselt logisid, hinnatakse süsteemide koormust ja reageeritakse ilmnevatele probleemidele. Samuti tuleb jälgida, et varundusprotsessid toimiksid automaatselt ja vastavalt ajakavale, ning et seotud tegevused oleksid dokumenteeritud.
       7. Taasteprotsesside tõhusust hinnatakse taastetestide abil, keskendudes eelkõige kriitilistele süsteemidele ja andmetele, lähtudes riskihinnangutest. Testimine toimub vähemalt kord aastas ning tulemused dokumenteeritakse süsteemide dokumentatsioonis. Vajadusel viiakse ellu parandusmeetmed.
       8. Taasteplaanid koostatakse riskihinnangute alusel nende süsteemide jaoks, millel on ülikooli toimimise seisukohalt oluline või kriitiline roll. Taasteplaan peab määratlema taastamisprotseduurid, vastutavad isikud ning taasteaja (RTO) ja taastepunkti (RPO) eesmärgid. Plaanis kajastatakse ka turvalahendused taasteks vajalike paroolide ja krüptovõtmete käsitlemiseks ning alternatiivsed taastamisvõimalused olukordadeks, kus esmased ressursid pole kättesaadavad.
       9. Süsteemihaldur vastutab varundus- ja taasteprotsesside toimimise, dokumenteerimise ja ajakohasuse eest, tagades vastavuse nii organisatsiooni sisemistele nõuetele kui ka asjakohastele standarditele.
   12. **Infosüsteemide, virtuaalserverite ja füüsiliste serverite sulgemine ning kasutuselt kõrvaldamine**
       1. Infosüsteemide ja serverite elutsükli lõppfaas tuleb korraldada läbimõeldult, et säiliks usaldusväärsus, andmete käideldavus ja teenuste järjepidevus. Käesolev punkt kirjeldab standardseid põhimõtteid infosüsteemide sulgemiseks, virtuaalserverite peatamiseks ning füüsiliste serverite kasutuselt kõrvaldamiseks. Täpsemad juhised ja tehnilised sammud määratletakse eraldi protseduurides ja tööjuhistes.
       2. Infosüsteemi sulgemine algab vajaduse hindamisest ja kavandamisest koostöös süsteemi omaniku ja vastutavate osapooltega. Sulgemisprotsess peab hõlmama andmete ja logide säilitamist või arhiveerimist vastavalt organisatsiooni säilituspõhimõtetele, kasutajakontode ja õiguste sulgemist ning sõltuvuste ja liidestuste kaardistamist. Kui süsteem ei ole enam kasutusel või selle teenused viiakse üle teisele platvormile, lõpetatakse toimingud etappide kaupa. Sulgemine dokumenteeritakse koos põhjenduse, kuupäeva, säilitamisotsuste ja vastutajatega.
       3. Seotud virtuaalserveri sulgemine toimub pärast infosüsteemi sulgemist. Enne virtuaalserveri kustutamist tuleb veenduda, et vajalikud andmed, konfiguratsioonid ja logid on kopeeritud või arhiveeritud ning et server ei ole seotud ühegi aktiivse teenusega. Virtuaalkettad ja salvestusseadmed, mis sisaldavad tundlikku teavet, puhastatakse turvalise meetodi abil ning toiming logitakse koos serveri identifikaatorite ja kuupäevaga. Ressursid vabastatakse alles pärast seda, kui vajalikud kontrollid on läbitud ja sulgemine kinnitatud.
       4. Füüsilise serveri kõrvaldamine toimub siis, kui see ei majuta enam ühtegi toimivat süsteemi ega virtualiseerimiskeskkonda. Andmekandjad puhastatakse või hävitatakse turvaliselt, seadmetelt eemaldatakse varade sildid ja muud identifitseerivad andmed. Toiming dokumenteeritakse koos kuupäeva, hävitamismeetodi ja vastutajaga. Kui kõrvaldamisega tegeleb väline teenusepakkuja, lisatakse dokumentatsiooni ka vastavad kinnitused või vastuvõtutõendid. Füüsilise kõrvaldamise korraldamine peab toimuma vastavuses organisatsiooni andmeturbe- ja varahalduspõhimõtetega.
       5. Sulgemise ja kõrvaldamisega seotud tegevused dokumenteeritakse viisil, mis tagab jälgitavuse ja auditeeritavuse. Protsessi eest vastutavad määratud süsteemi- ja varahaldurid, kelle ülesanne on koordineerida toimingud ning tagada nõuetekohane läbiviimine.
   13. **Dokumenteerimine**
       1. Serverite, infosüsteemide ja infotehnoloogiliste varade dokumentatsioon hallatakse keskse platvormina (hetkel *Confluence*), kuhu koondatakse nii üld- kui käidudokumentatsioon. Vajadusel võib keskne platvorm muutuda, kuid dokumenteerimise põhimõte jääb samaks. Dokumentatsioon hõlmab süsteemide konfiguratsioone, turvanõudeid, haldusjuhiseid ja muid protsesse, mis on vajalikud toimimiseks, haldamiseks ja järelevalveks.
       2. Dokumentatsioon peab olema ajakohane ning käsitlema vähemalt järgmisi teemasid:
          1. riistvaralised hooldus- ja asendustoimingud, sealhulgas komponentide elutsükli haldus;
          2. ligipääsuõiguste haldamise ja auditeerimise kirjeldus, sh õiguste määramine, ülevaatus ja eemaldamine;
          3. intsidentide ja süsteemirikete käsitlemise juhised;
          4. infosüsteemide ja rakenduste konfiguratsioonid ning liidestuste kirjeldused;
          5. varundamise ja taastamise juhendid, sh testide läbiviimise metoodika.
       3. Konfiguratsioonimuudatused dokumenteeritakse muudatuste halduse protseduuride kohaselt ning peavad olema jälgitavad ja auditeeritavad. Dokumenteerimiseks kasutatakse lisaks kesksele platvormile ka teisi töövahendeid, näiteks *VMware’i, GitLabi/GitHubi, Jira varahaldust või Automoxi,* mis loovad või haldavad teatud infot vaikimisi. Nendes keskkondades tekkivat dokumentatsiooni ei dubleeritud eraldi, vaid seda kasutatakse viidete kaudu. Loetelu töövahenditest ei ole lõplik ja võib aja jooksul muutuda, mis tähendab, et dokumenteerimise põhimõtted kehtivad ka tööriistade vahetumise korral.
       4. Dokumentatsioonikeskkondade sisu vaadatakse korrapäraselt üle ja ajakohastatakse. Süsteemihaldurid vastutavad enda hallatavate süsteemide ja varade dokumentatsiooni terviklikkuse ja täpsuse eest ning osalevad regulaarsetes auditites, et vältida kõrvalekaldeid infoturbepoliitikast ja tagada vastavus standarditele.
   14. **Järelevalve ja auditeerimine**
       1. Serverihalduse vastavust kehtestatud nõuetele hinnatakse regulaarselt vastavalt ülikooli infoturbe riskihalduse põhimõtetele. Auditid ja turvaskaneeringud toimuvad määratud intervallidega, et ennetada ja tuvastada turvahaavatavusi ning konfiguratsioonivigu.
       2. Infoturbejuht koos infoturbetiimiga jälgib varundusprotsesside vastavust regulatiivsetele nõuetele ning hindab riske, ajakohastades varundamispoliitikat vajaduse korral. Samuti tagatakse, et krüpteerimis- ja muude turvakontrollide rakendamine on korrektne, vältimaks volitamata juurdepääsu ja andmeleket.
       3. Auditite ja skaneeringute tulemused dokumenteeritakse ja analüüsitakse, et võimaldada kiire reageerimine ning vajadusel ennetavate meetmete rakendamine.
       4. Eeskirja rikkumise korral rakendatakse asjakohaseid sanktsioone, sealhulgas hoiatusi, juurdepääsu piiramist, töösuhte lõpetamist või muid õiguslikke meetmeid. Eeskirja sisu vaadatakse üle vähemalt kord aastas, arvestades tehnoloogia, regulatsioonide ja kasutusvajaduste muutumist.
3. **Võrguhaldus**
   1. Ülikooli võrguhaldus peab tagama IT taristu töökindluse, turvalisuse ja kättesaadavuse. Võrguhalduse eesmärk on tagada turvaline andmeside, optimeeritud jõudlus ning kaitse võimalike ohtude ja rikkumiste eest.
   2. Ülikooli võrgu infrastruktuuri arendamisel, kavandamisel ja haldamisel tuleb lähtuda turvanõuetest, süsteemi töökindlusest ja tulevikuvajadustest. Võrgu arendamine peab tagama süsteemi pikaajalise jätkusuutlikkuse, kavandamine peab toetama tõhusat haldust ning haldamine peab tagama võrgu stabiilsuse, turvalisuse ja sujuva toimimise. Võrgu planeerimise, arenduse ja haldustegevused peavad vastama ülikooli strateegilistele eesmärkidele ning toetama akadeemilisi ja haldusprotsesse.
   3. **Võrgu arendamine**
      1. Võrgulahenduse arendamisel lähtutakse parimatest praktikatest ja uuematest tehnoloogiatest, et tagada süsteemi turvalisus ja pikaajaline jätkusuutlikkus. Rakendatavad lahendused peavad toetama ülikooli strateegiat ning teadus-, õppe- ja haldustegevusi.
      2. Võrgulahendusi hinnatakse ja uuendatakse regulaarselt vastavalt turvanõuetele ja tehnoloogia arengule, et tagada süsteemi tõhusus ja töökindlus. Uuendused kavandatakse viisil, mis ei katkestaks kriitilisi teenuseid.
      3. Riskihaldus toimub ülikooli infoturbe riskihaldusjuhise alusel. Turvauuendused ja tehnilised täiustused rakendatakse regulaarselt. Enne uute lahenduste kasutuselevõttu viiakse läbi testimine, et vältida haavatavusi ja tagada sujuv liidestamine olemasoleva süsteemiga.
   4. **Võrgu kavandamine ja projekteerimine**
      1. Võrguhalduse kavandamisel lähtutakse ülikooli infoturbepoliitikast, tööülesannetest ja vajalikest juurdepääsuõigustest. Arvesse võetakse halduseks eraldatud võrgualad, juurdepääs haldusserveritele, andmesideprotokolle, sündmuste- ja alarmiteadete liidesed ning keskne logimislahendus.
      2. Võrk peab olema modulaarne, et tagada loogiline haldus, turvalisus ja paindlikkus. Segmenteerimine peab eraldama tundlikud andmed avalikest teenustest, vähendades turvariske. Andmeliiklust ja koormust tuleb optimeerida, et vältida ülekoormust ja tagada teenuste toimivus. Uued lahendused hinnatakse eelnevalt turvariskide ja ühilduvuse osas. Võrguhalduse nõuded, sh haldusvahendite ja -protsesside kirjeldused, dokumenteeritakse kavandamise käigus.
   5. **Võrguarhitektuur ja segmentatsioon**
      1. Ülikooli võrk on jaotatud turvatasemepõhisteks kaitsetsoonideks, mille sees paiknevad võrgusegmendid *(VLAN-id)* vastavalt kasutajarollidele ja teenuste funktsioonidele.
      2. Igal tsoonil ja segmendil on kindel eesmärk ning sellele vastavad turbe- ja juurdepääsunõuded. Need määravad, millised seadmed, teenused või kasutajad vastavas alas paiknevad, ning on kirjeldatud võrgu dokumentatsioonis, mida kasutatakse juurdepääsude kavandamisel ja kontrollimisel.
      3. Tsoonide ja segmentide vaheline liiklus on vaikimisi keelatud. Suhtlus on lubatud üksnes dokumenteeritud ja vajaduspõhiste reeglite alusel. Lubatud ühendused peavad vastama turvanõuetele ning toetama ülikooli tegevusvajadusi.
      4. Segmenteerimist ja juurdepääsupiiranguid vaadatakse regulaarselt üle ning ajakohastatakse vastavalt tehnoloogia arengule, riskihindamisele ja struktuurimuudatustele. Hästi korraldatud segmenteerimine toetab võrgu töökindlust, turvalisust ja haldamist.
   6. **Võrgu haldamine**
      1. Ülikooli IT osakond vastutab võrgu infrastruktuuri haldamise, monitoorimise ja turvalisuse eest. Eesmärk on tagada süsteemi töökindlus, järjepidevus ja kaitse võimalike ohtude eest.
      2. Võrguressursside kasutamine ja juurdepääs peavad olema kontrollitud ja logitud, et vältida volitamata ligipääsu ning võimaldada turvaintsidentide tuvastamist ja uurimist.
      3. Ülikooli võrku ei tohi iseseisvalt ühendada võrguseadmeid (nt switch, tulemüür, WiFi pääsupunkt). Sellised ühendused on lubatud üksnes IT osakonna eelneval kooskõlastusel ning põhjendatud juhtudel, näiteks teadustööks. IT osakonnal peab olema täielik ülevaade võrgu komponentidest, et tagada turvalisus, töökindlus ja probleemide kiire lahendamine.
      4. Võrgutaristu peab olema pideva järelevalve all, et ennetada rikkumisi ja tagada süsteemi stabiilsus. Muudatused ja hooldused dokumenteeritakse ning viiakse läbi vastavuses muudatuste halduse protsessiga. Võrguhalduse põhimõte on: kõik mittevajalik tuleb keelata. Haldustegevused toimuvad kaitstud kanalite kaudu ning andmesideks kasutatakse ainult turvalisi protokolle.
      5. Haldusvõrgu komponentide tarkvara, püsivara ja konfiguratsioonid peavad olema keskselt hallatud ning võimalikult suures osas automatiseeritud. Konfiguratsioonimuudatused ei tohi põhjustada ootamatuid katkestusi. Seadistused tuleb hoida turvaliselt ja kättesaadavana üksnes volitatud töötajatele. Konfiguratsioonihaldus peab olema seotud versioonihalduse ja varundusprotsessidega ning seadistused tuleb regulaarselt varundada.
      6. Konfiguratsioonid ja võrguseadmete haldusandmed kuuluvad taasteplaanidesse. Varundamine ja taasteprotsessi testimine toimub perioodiliselt, et tagada taastamisvõimekus.
      7. Seadistused peavad vastama turvalise algseadistuse *(secure baseline configuration)* nõuetele. Vaikekasutajad, vaikeseadistused ja mittevajalikud teenused tuleb keelata. Konfiguratsioonifailid ja ligipääsuvõtmed hoitakse krüpteeritult ning kaitstuna volitamata muutuste eest.
      8. Võrgukonfiguratsioone ja haldusmeetmeid vaadatakse regulaarselt üle ja ajakohastatakse. Seadmete hooldus ning tarkvarauuendused viiakse läbi vastavalt kehtestatud ajakavale. Turvapaigad rakendatakse viivitamatult pärast valideerimist, et vähendada riske ja tagada süsteemi ajakohasus.
      9. Võrguga seotud töötajad ja administraatorid peavad regulaarselt läbima infoturbekoolitusi. Koolituste eesmärk on suurendada teadlikkust turvaohtudest, ennetus- ja reageerimismeetmetest ning tagada turvaliste seadistus- ja halduspraktikate järgimine.
   7. **Võrgu juurdepääsukontrolli rakendamine ja autentimisnõuete järgimine**
      1. Ülikooli võrgu ja IT süsteemide turvalisuse tagamiseks tuleb rakendada tõhus juurdepääsukontroll, mis piirab ja haldab ligipääsu vastavalt kasutajate rollidele ja tööülesannetele. Autentimis- ja autoriseerimismeetmed peavad tagama, et süsteemidele, andmetele ja võrgule pääsevad ligi ainult volitatud kasutajad ning ligipääsud on kontrollitud ja auditeeritavad.
      2. Autentimine on nõutav enne juurdepääsu saamist sisemistes kaitsetsoonides ja võrgusegmentides paiknevatele teenustele. Lähtudes riskihinnangust ja tehnilisest võimekusest liigub ülikool kasutajapõhise autentimise ja autoriseerimise suunas, asendades IP-aadressipõhist juurdepääsukontrolli seal, kus tegemist on inimkasutajate ligipääsuga. See ei ole kohustuslik kõikides olukordades, vaid rakendub eelkõige juhtudel, kus see on otstarbekas ja riskijuhtimise seisukohalt põhjendatud. IP-põhine kontroll on siiski asjakohane süsteemide ja teenuste vahelise suhtluse puhul, näiteks andmevahetuseks ja automaatseks koostööks sisemiste komponentide vahel, kui see on tehniliselt põhjendatud ja vastab turvanõuetele.
      3. Juurdepääsuhalduse protsess ja nõuded on reguleeritud ülikooli korras „Infotehnoloogilistele varadele juurdepääsuhaldus“, mis sätestab detailse protsessi kasutajate ja kolmandate osapoolte ligipääsu haldamiseks ja kontrollimiseks.
      4. Ligipääsuõigused määratakse minimaalse vajalikkuse põhimõttel – kasutajale antakse ligipääs üksnes nendele ressurssidele, mis on vajalikud tööülesannete täitmiseks. Õiguste määramised, muudatused ja erandid dokumenteeritakse ning peavad olema põhjendatud vastavalt kehtivale juurdepääsukorrale.
      5. Tundlike süsteemide ja võrguteenuste kasutamine peab toimuma turvaliste ühenduste kaudu, mis välistavad volitamata ligipääsu ja andmelekked. Kaugühenduste puhul tuleb kasutada tugevat autentimist ning krüpteeritud andmesidekanaleid. Võrguhaldus peab seejuures olema selgelt eraldatud, paiknedes omaette turbetsoonis ja spetsiaalses võrgusegmendis, kuhu pääsevad üksnes volitatud administraatorid. Otseühendused kriitiliste komponentidega ei ole lubatud – haldus toimub piiratud juurdepääsuga hüppeserveri kaudu. Kui halduspääs on vajalik väljastpoolt ülikooli võrku, tuleb see suunata turvatud kanalisse (nt VPN), mis viib hüppeserverini ja tagab kontrollitud, logitava ning auditeeritava juurdepääsu.
      6. Autentimis- ja autoriseerimissüsteemid peavad olema pideva järelevalve all, et tuvastada kahtlasi tegevusi ja reageerida kiiresti. Juurdepääsureeglite ja autentimisprotsesside regulaarne ülevaatus aitab kõrvaldada aegunud või mittevajalikud õigused.
      7. Autentimisprotsessid ja juurdepääsuõigused dokumenteeritakse ning peavad olema kooskõlas ülikooli infoturbe- ja andmekaitsepoliitikaga, et tagada läbipaistvus ja kehtivatele turvanõuetele vastamine.
   8. **Võrgu andmeliikluse monitooring ja anomaaliate tuvastamine**
      1. Ülikooli võrgu infrastruktuur peab olema pideva järelevalve all, et tuvastada võimalikke turvaohtusid, anomaaliaid ja ebatavalisi tegevusi. Võrguseadmed ja kriitilised teenused peavad olema jälgimisel, et ennetada rikkeid, reageerida turvaintsidentidele ning tagada võrgu töökindlus ja turvalisus.
      2. Võrgumonitooringus kasutatakse tulemüüre ning sissetungi tuvastamise süsteeme, mis võimaldavad leida ja blokeerida kahtlase tegevuse ning ennetada pahatahtlikke rünnakuid. Võrgu juurdepääsureeglid peavad olema selgelt määratud ning kõik volitamata ühendused tuleb blokeerida.
      3. Oluliste võrgukomponentide käideldavus- ja sooritusparameetreid tuleb jälgida reaalajas ning määrata sobivad seireparameetrid, mis dokumenteeritakse. Võrguliikluse mustreid ja koormust analüüsitakse pidevalt, et tuvastada ebatavalist tegevust ja võimalikke ründeid.
      4. Turvaskaneeringud ja auditid tuleb läbi viia regulaarselt, et avastada haavatavusi ning tagada süsteemi vastavus kehtivatele infoturbe- ja regulatiivnõuetele. Võrguturbeintsidentide käsitlemiseks peab olema kehtestatud selge protseduur, mis hõlmab intsidentide tuvastamist, analüüsi, reageerimist ja parandusmeetmete rakendamist. Intsidendid dokumenteeritakse ning vajadusel teavitatakse asjakohaseid osapooli vastavalt ülikooli küberturbe- ja andmekaitsepoliitikale.
      5. Turvaintsidentide lahendamisel peab IT osakond järgima kindlaksmääratud protokolle ning rakendama meetmeid, mis tagavad kiire reageerimise ja intsidendi mõju minimeerimise. Intsidentide käsitlemisel lähtutakse ülikooli korrast "Pöördumiste, intsidentide, sündmuste ja probleemide haldus", mis sätestab ka intsidentide analüüsi ja ennetavate meetmete rakendamise korra.
   9. **Võrguhalduse dokumentatsioon ja juhend**
      1. Võrgu turvalise, töökindla ja hallatava toimimise tagamiseks peavad olema kirja pandud kriitilised elemendid, mis puudutavad võrgu ülesehitust ja haldust. Dokumentatsioon aitab tagada tegevuste läbipaistvuse, tõrgete ennetamise ning kiire reageerimise olukordades, kus on vaja teha muudatusi, tõrkeotsingut või taastamist.
      2. Dokumenteeritud peavad olema võrgu arhitektuur ja topoloogia, sealhulgas kaitsetsoonid, võrgusegmendid, kriitilised seadmed ja ühenduspunktid. Samuti tuleb kirja panna tsoonide vahelise liikluse reeglid ning kasutajate, teenuste ja seadmete paiknemise loogika.
      3. Juurdepääsude haldus peab olema selgelt kirjeldatud: kes, millele ja kuidas ligi pääseb. Kirjas peavad olema autentimisviisid, juurdepääsuõiguste määramise põhimõtted ja erilahendused, näiteks hüppeserveri või VPN-i kasutamine.
      4. Haldusprotseduurid, nagu konfiguratsioonide muutmine, juurdepääsu andmine ja halduskanalite kasutamine, tuleb samuti dokumenteerida.
   10. **Järelvalve** 
       1. Võrguhaldusele esitatud nõuetele vastavuse tagamiseks tuleb regulaarselt hinnata dokumentatsiooni ajakohasust, selle vastavust tegelikule olukorrale ning kehtivatele protseduuridele. Järelvalve käigus kontrollitakse, kas võrguhalduse taristu on turvaline, jätkusuutlik ja vastab kehtestatud turvanõuetele.
       2. Võrguhalduse järelvalve on pidev ja süsteemne protsess, mille eesmärk on ennetada võimalikke turvariske ja tagada võrgu tõrgeteta toimimine. Järelvalvet teostatakse regulaarsete ülevaatuste ja auditite kaudu, lähtudes ülikooli infoturbe- ja halduspoliitikatest. Järelvalve tegevused ei pruugi vajada eraldi kontrolltoimingu märget, kuid olulised tähelepanekud ja parandust vajavad aspektid dokumenteeritakse ning nende lahendamiseks rakendatakse vastavaid meetmeid.