JYVÄSKYLÄN YLIOPISTO

VARMENNUSTOIMINNAN TILA

13.3.2024

SISÄLLYS

1. TAUSTA

Jyväskylän yliopiston hallitukselle on aiemmin raportoitu tietotilinpäätös, laadunhallinnan tila sekä turvallisuuskatsaus erillisinä tarkasteluina. Vuonna 2023 raportointi toteutettiin ensimmäistä kertaa kokonaisuutena, mikä kattaa laajemmin varmennustoiminnan eri osa-alueet.

Varmennustoiminnalla tarkoitetaan yliopiston toiminnan ja sen suunnittelun laadukkuuden, turvallisuuden, vaatimustenmukaisuuden ja tuloksellisuuden varmistamista. Varmennustoiminnan käsitettä käytetään kattokäsitteenä, joka nivoo laadunhallinnan, riskienhallinnan, turvallisuuden, tietosuojan ja tietoturvallisuuden sekä sisäisen tarkastuksen saman kokonaisuuden ympärille. Kutakin osa-aluetta ohjaa kansainväliset standardit, normit tai toimintaperiaatteet, joita on hyödynnetty Jyväskylän yliopiston varmennustoiminnan politiikkaa ja periaatteita määritettäessä.

Varmennustoiminta tukee yliopiston strategista ja operatiivista johtamista. Se auttaa yliopistoa saavuttamaan tavoitteitaan, toimimaan turvallisesti, vastuullisesti ja eettisesti sekä mahdollistaa yliopistoon kohdentuvien riskien hallitsemisen. Varmennustoiminnalla huolehditaan lisäksi sisäisen valvonnan toimivuudesta sekä toiminnan oikeellisuudesta.

Varmennustoiminta koskee Jyväskylän yliopistoa ja sen alaisia yksiköitä (tiedekunnat, erillislaitokset, laitokset ja yliopistopalvelut). Varmennustoiminta liittyy yliopisto-, yksikkö- ja yksilötason toimintaan.

Raportin on tarkoitus luoda yliopiston hallitukselle sekä muille yliopistoyhteisössä toimiville elimille ja yhteisön jäsenille kokonaiskuvaa yliopiston varmennustoiminnan tilasta. Raporttia voi hyödyntää perehtymällä kokonaisuuteen tai ainoastaan tiettyyn osa-alueeseen, jotka ovat selkeästi eroteltuja osioita. Varmennustoimintaa ohjataan varmennustoiminnan politiikka ja periaatteet -asiakirjalla, joka on hyväksytty yliopiston hallituksessa 19.1.2024.

Raportti kattaa varmennustoiminnan osalta seuraavat näkökulmat:

- laadunhallinta
- riskienhallinta
- turvallisuus
- työsuojelu
- tietoturva
- tietosuoja

Sisäisestä tarkastuksesta raportoidaan yliopiston hallitukselle erillisessä dokumentissa.

Yliopiston arvot ovat avoimuus, luottamus, laatu ja eettisyys. Varmennustoiminta tukee näiden arvojen mukaista toimintakulttuuria.

2. VARMENNUSTOIMINTA JYVÄSKYLÄN YLIOPISTOSSA

Jyväskylän yliopistossa on varmennustoimintaa kehitetty aktiivisesti vuodesta 2022 alkaen. Kehitystyö jatkuu vielä vuoden 2024 lopulle, minkä jälkeen tavoitteena on toiminnan vakiinnuttaminen organisaation eri tasoille.

Jyväskylän yliopistossa on laadittu vuoden 2023 aikana varmennustoiminnan politiikka ja periaatteet (hyväksytty hallituksessa 19.1.2024), mikä yhdenmukaistaa ja ohjaa varmennustoimintaa koko yliopistossa.

Varmennustoiminta muodostuu eri osa-alueista, ja syksystä 2021 alkaen yliopistotasoista varmennustoimintaa on koordinoitu monialaisessa varmennustoiminnan tiimissä, mikä on mahdollistanut eri näkökulmien välisen synergian ja toiminnan kokonaisvaltaisen kehitystyön. Lisäksi yliopistossa toimivat laadunohjausryhmä, riskienhallintaryhmä sekä tietoturvan- ja tietosuojan kehittämisryhmä, joilla on tärkeä asiantuntijarooli näiden osa-alueiden kehittämisessä ja operatiivisen toiminnan ohjauksessa.

Keskeiset nostot vuodelta 2023 ja alkuvuodesta 2024

- Saatu valmiiksi varmennustoiminnan politiikka ja periaatteet -asiakirja.
- Sisäinen tarkastus on kilpailutettu ja valittu palvelun tuottajaksi BDO. Uuden toimintamallin mukainen sisäinen tarkastustoiminta on aloitettu.
- Varmennustoimintaa johdetaan ja koordinoidaan yhtenä kokonaisuutena ja henkilöstöä on keskitetty organisaatiossa.
- On tehty kriittisiä henkilöstörekrytointeja sekä lisätty asiantuntijoiden määrää yliopisto- ja yksikkötasolla.
- Riskienhallinnan ja turvallisuuden digitaalinen Rego-ohjelmisto on otettu käyttöön.
- Kriittiseen viestintään ja hälyttämiseen tarkoitettu Secapp-sovellus on käyttöönottovaiheessa pilottina.
- On kehitetty laadunparantamisen tueksi tiedollatoimimisen ja -johtamisen edellytyksiä.
- Riskienhallinnan ja turvallisuuden operatiivinen koordinaatioryhmä on asetettu helmikuussa 2024. Ryhmä käsittelee erityisesti turvallisuuteen liittyviä havaintoja, ja pyrkii nopeuttamaan mahdollisten epäkohtien kuntoon laittamisen läpimenoaikaa.

Keskeiset havainnot varmennustoiminnan kannalta

- Vaikka yliopiston organisaatiokulttuuri ei kaikilta osin tue turvallisuuden ja riskienhallinnan edistämistä tai kaikilta osin jatkuvaa laadun parantamista, yliopistoyhteisössä on kuitenkin myönteinen suhtautuminen toiminnan kehittämiseen ja siihen resursoimiseen.
- Yhteenvetona voidaan todeta, että varmennustoiminnan resursointi on oikein mitoitettu, sekä vuonna 2022 aloitetun kehitystyön jälkeen on tärkeää vakiinnuttaa luodut toimintamallit yliopistoyhteisöön. Kriittinen menestystekijä on esihenkilöroolien ja vastuiden määrittely ja selkiyttäminen sekä roolien mukaisten tehtävien hoitaminen.

3. VARMENNUSTOIMINNAN TILA

3.1 Laadunhallinta

3.1.1 Laadunhallinta Jyväskylän yliopistossa

Jyväskylän yliopiston varmennustoiminnan politiikan mukaan laadunhallinnalla tarkoitetaan menettelytapoja ja prosesseja, joiden avulla yliopisto suunnittelee, toteuttaa, ylläpitää, seuraa ja arvioi sekä kehittää toimintaansa ja sen laatua (STAK/PDCA-kehä). Hyvä laadunhallinta on osa kaikkea yliopiston toimintaa ja sen avulla vahvistetaan jatkuvaan laadun parantamiseen tähtäävää toimintakulttuuria.

Laadunhallinnan tulisi olla kiinteä osa strategista ja operatiivista johtamista ja toiminnan ohjausta. Yliopiston laatutyö kattaa yliopiston perustehtävät tutkimuksen ja koulutuksen, niihin perustuvan yhteiskunnallisen vuorovaikutuksen sekä ydintehtäviä tukevat palvelut. Laadunhallinnan tavoitteena on tukea yliopiston perustehtäviä ja sitä kautta edistää yliopiston toiminnalleen asettamien tavoitteiden saavuttamista.

Laadunhallinnan kokonaisuudella tarkoitetaan laadunhallinnan organisoinnista, vastuunjaosta, vakiintuneista toimintatavoista ja resursseista muodostuvaa systemaattista kokonaisuutta. Laadunhallinnan menettelyin yliopisto ohjaa yhteisöään varmistamaan toiminnan laadun ja sen jatkuvan kehittämisen.

Toimivan laatujärjestelmän tavoitteena on

- turvata toiminnan yhdenmukaisuus ja oikeudenmukaisuus jaettujen ja avoimien toimintatapojen, toimintamallien ja määriteltyjen vastuiden kautta
- parantaa yliopiston kykyä saavuttaa tavoitteet, seurata tavoitteiden toteutumista, puuttua poikkeamiin sekä tukea toiminnan kehittämistä
- luoda avointen palautekäytäntöjen avulla keinot yhteisön vaikuttamiselle ja kuulluksi tulemiselle
- varmistaa, että organisaatiossa on sovitut vastuut ja menettelyt yhteisesti sovittujen asioiden toteuttamiseen ja muutosten vaikutusten seurantaan
- tukea johtamista tuottamalla tietoa päätöksenteon tueksi
- tukea avoimuuteen ja dialogisuuteen perustuvan toimintakulttuurin rakentumista
- edistää toiminnan suunnitelmallisuutta ja järjestelmällisyyttä

Laatujärjestelmän tarkoituksena on tukea kolmea laadunhallinnan osa-aluetta, laadun suunnittelua, laadun varmistusta sekä laadun kehittämistä ja parantamista. Laadun suunnittelua on muun muassa systemaattisten toimintamallien, menettelytapojen ja periaatteiden määrittely, jotka ohjaavat toimintaa.

Yliopiston keskeinen laadunvarmistuksen menettelytapa on arviointi. Arviointimenettelyinä käytetään sisäisiä auditointeja ja itsearviointeja sekä asiantuntijoiden tai asiantuntijaryhmien tekemiä ulkoisia arviointeja. Yliopisto osallistuu yliopistolain velvoittamana Karvin toteuttamaan laatujärjestelmän toimivuuden auditointiin kuuden vuoden välein.

Laadun parantamiseen tähtäävä kehittäminen on jatkuva prosessi, jossa suunnittelu, toiminta, arviointi ja kehittäminen seuraavat toisiaan. Hallittu ja systemaattinen toiminnan kehittäminen tukee jatkuvan laadun parantamisen kulttuurin rakentumista. Laadun parantamisen keskeinen toimintatapa on tietoon, palautteeseen ja arviointeihin perustuva toiminnan ja toimintatapojen kehittäminen.

3.1.2 Keskeiset tapahtumat edellisen raportin jälkeen

Laatujärjestelmän kehittäminen

Tiedolla toimimisen edellytyksiä vahvistettiin uusilla keskitetysti tuotettavilla raporttikokonaisuuksilla, jotka jaetaan PowerBI-alustalla. Yksiköiden johdon käyttöön julkaistiin toukokuussa 2023 talouden raportit, jotka automatisoivat ja visualisoivat aiemmin käsin tuotettuja raportteja. Täydentävän rahoituksen projektien ja sisäisten tilausten vastuuhenkilöiden käyttöön julkaistiin raporttikokonaisuus näiden projektien talouden seurantaan.

Vuoden aikana Avoimen yliopiston tuottamasta koulutuksesta suunniteltiin Sisu-raportointi. Myös toteutus alkoi vuoden 2023 puolella. Raportointikokonaisuuden tavoitteena on automatisoida ja visualisoida koulutuksen toteuttamiseen liittyvää tietoa sekä operatiivisen että strategisen johtamisen tueksi. Raportoinnin kehittämisen yhteydessä tehtiin raportoinnin suunnittelu- ja toteutusprosessiin kuuluvana lähdejärjestelmän datan ja datan syntymisen osalta prosessien oikeellisuuden laadunvarmistus.

Vuoden aikana tuotettiin konsepti Tilannekartasta (aikaisemmin nimellä johdon dashboard) ja toteutus käynnistettiin vuoden lopulla. Tilannekartta on johtamisen tueksi rakennettava digitaalinen ja visuaalinen tilannekuvanäkymä, joka tulee yhdistämään monesta eri lähdejärjestelmästä kokoavaa ja johtamisen kannalta merkityksellisintä tietoa yliopisto- ja yksikkötasolla.

Laadun suunnittelu ja ohjaus

Jyväskylän yliopistossa otettiin käyttöön ilmoittajansuojalain mukainen väärinkäytösten whistleblowing-ilmoituskanava maaliskuussa 2023. Kanavan tarkoituksena on tukea yliopiston eettisten periaatteiden ja arvojen toteutumista sekä tarjota työkalu väärinkäytösten ilmoittamiseen.

Hallitus vahvisti tutkintosäännön päivityksen maaliskuussa 2023. Tutkintosäännön päivittämiselle havaittiin tarvetta vuonna 2022 mm. Avoimen yliopiston muuttuneen organisaatiorakenteen vuoksi ja muita päivitystarpeita kartoitettiin kokoamalla niitä koulutusneuvostolta, tiedekuntien ja erillislaitosten koulutuksesta vastaavilta varajohtajilta sekä opintopäälliköiltä.

Koulutusneuvosto käynnisti yliopiston Opiskelun eettiset ohjeet ja vilppitapausten käsittely -periaatteiden päivittämisen. Aikaisempi päätös opiskelun eettisen ohjeiden ja vilppitapausten käsittelystä on vuodelta 2019. Rehtori vahvisti vilppitapausten käsittelyn periaatteet kesäkuussa 2023.

Koulutusneuvosto käynnisti opetussuunnitelmaprosessin yhteydessä laadukkaan ohjauksen periaatteiden päivittämisen. Laadukkaan ohjauksen periaatteet ohjaavat laitos- ja

yksikkökohtaiset ohjauksen toteuttamissuunnitelmien laatimista, jotka astuvat voimaan samanaikaisesti uusien opetussuunnitelmien kanssa. Koulutuksesta vastaava vararehtori vahvisti Laadukkaan ohjauksen periaatteet syyskuussa 2023.

Yliopistossa käynnistettiin valmistelu tutkimuksen ja tutkijan vastuullisen arvioinnin periaatteiksi, jotka tulevat ohjaamaan sitä, miten Jyväskylän yliopistossa arvioidaan tutkijoiden työtä. Valmistelu toteutettiin henkilöstöpalveluiden, Avoimen tiedon keskuksesta ja tutkimus- ja innovaatiopalveluiden yhteistyönä ja valmistelussa otettiin huomioon kansalliset ja kansainväliset periaatteet ja julistukset, joiden noudattamiseen yliopisto on sitoutunut. Rehtori hyväksyi tutkimuksen ja tutkijan vastuullisen arvioinnin periaatteet joulukuussa 2023.

Hallitus käynnisti alkuvuodesta varmennustoiminnan asiakirjakokonaisuuden päivitys- ja uudistamisprosessin. Yliopistolta puuttui periaatelinjaukset, toimintamalli ja ohjeistukset riskienhallinnasta. Valmistelussa päädyttiin yhdistämään laatupolitiikka, turvallisuuspolitiikka sekä myös sisäisen tarkastuksen toteuttamisestä ohjaava varmennustoiminnan ohjesääntö uuden riskienhallinnan sisällön kanssa yhdeksi kokonaisvaltaiseksi asiakirjaksi. Tietoturvaa ja tietosuojaa koskevat asiakirjat jätettiin omiksi asiakirjoikseen. Hallitus hyväksyi Varmennustoiminnan politiikka ja periaatteet -asiakirjan tammikuussa 2024.

Sisäisen tarkastuksen toteutusmalli uudistettiin vuoden 2023 aikana, ja sisäinen tarkastus toteutetaan kilpailutetun ulkoisen yhteistyökumppanin kanssa yliopiston sisäisen tarkastajan eläköidyttyä. Sisäisten tarkastusten suunnittelu toteutetaan varmennustoiminnan politiikan ja periaatteiden mukaisesti. Sisäisen tarkastuksen pohjalta muodostettavien kehittämistoimenpiteiden uudistuva yliopiston sisäinen seurantaprosessi on vielä määrittelemättä.

Yliopistolle laadittiin edellisenä vuonna toteutusta sisäisestä itsearvioinnista saatujen syötteiden perusteella saavutettavuussuunnitelma, jota OKM edellytti yliopistoilta. Rehtori hyväksyi saavutettavuussuunnitelman tammikuussa 2023. Yhdenvertaisuus, saavutettavuus ja tasa-arvo kehittämisryhmä päivitti vuodelle 2024 Yhdenvertaisuus- ja tasa-arvosuunnitelman, jonka rehtori hyväksyi joulukuussa 2023.

Prosesseja kehitettiin Vasara-järjestelmään toteutettujen prosessien digitalisoinnin yhteydessä. Vasara-alusta on kehitetty Jyväskylän ylipistossa ja otettu käyttöön 2020 työnkulkujen digitalisoinnissa. Työnkulkujen automatisoinnilla tavoitellaan ajan säästöä ja tiedon laadun parantamista. Koulutustoiminnan osalta automatisoitiin seuraavia prosesseja: pilotoitiin opinnäytetöiden tarkastusprosessi, opinnäytteiden tarkastusprosessin ja JYX:n integraatio, lisäaikapäätösten valmistelu ja käsittely, erityispedagogiikan harjoitteluprosessin laajennus kaikkiin harjoitteluihin sekä ILPO-järjestelmään integroituvat tutkintoon johtamattomien opintojen haku- ja valintaprosessit. Tutkimustoiminnan ensimmäisenä prosessina digitalisoitiin tutkimusetiikkaan liittyvät lomakkeet ja mallipohjat eettisen lausuntopyynnön osalta. Lisäksi laajennettiin työsopimusprosessin digitalisointi koko yliopistoon, toteutettiin työnkulun automatisaatiot lausuntoprosessin ja tietosuojailmoituksen (aineistonhallinnan pilotti) osalta sekä jatkokehitettiin hankintapyynnön prosessia.

Laadunvarmistus

Vuoden aikana oli käynnissä suunnitellusti neljä arviointiprosessia.

Kansainvälinen JYU -itsearviointi toteutettiin tammikuussa 2023 laajan johtoryhmän vahvistamasta kolmesta kohdennetusta teemasta. Arviointiprosessin taustaksi laadittiin laaja yliopiston toimintaa läpileikkaavan kansainvälisyyden tila -raportti. Kehittämissyötteet on viety osaksi yliopiston strategiaohjausta ja toiminnanohjausta strategian virkistysprosessissa. Arviointiprosessista vastasi yliopiston johtoryhmä.

Tutkimuksen ulkoinen arviointi toteutettiin suunnitellusti vuoden 2023 aikana. Kevään itsearviointien pohjalta toteutettiin ulkoisen arviointiryhmän arviointivierailu toukokuussa 2023. Arviointi ja kehittämistoimenpiteet raportoitiin loppuvuodesta 2023. Arviointiprosessista vastasi tiedeneuvosto.

Jyväskylän yliopisto on sitoutunut Euroopan komission (EC) Human Resources Strategy for Researchers (HRS4R) -laatutyöhön vuodesta 2012. Prosessissa edistetään tutkijan uraa ja työskentelyedellytyksiä ja prosessi linkittyy vahvasti yliopistoyhteisö ja tutkimuksen kehittämisohjelmien päätavoitteisiin. Prosessiin kuuluu ulkoinen arviointi kolmen vuoden välein ja yliopiston 2022 itsearviointiin perustuva arviointipalaute saapui komissiolta huhtikuussa 2023 ja HR Excellence in Research -laatuleima on voimassa seuraavat kolme vuotta. Seuraava arviointivierailu toteutetaan kolmen vuoden päästä vuonna 2026. Prosessin ohjauksesta vastaa Osaava, luova ja hyvinvoiva yliopistoyhteisö -kehittämisryhmä.

Jyväskylän yliopisto hakeutui syksyllä 2022 yhdessä Jyväskylän Urheiluakatemian kanssa uuteen Olympiakomitean toteuttamaan Huippu-urheilijamyönteinen korkeakoulu -auditointiprosessiin. Prosessiin liittyvä itsearviointi toteutettiin keväällä, jonka pohjalta laadittiin itsearviointiraportti. Auditointivierailu toteutettiin marraskuussa 2023. Arviointiprosessin omistaa koulutusneuvosto.

Laadun parantaminen

Varmennustoiminnan seurantamenettelyssä (sisäisen tarkastuksen Audit Log -seuranta) oli neljä koulutuksen sisäistä itsearviointia, jotka on toteutettu vuosina 2019–2020: koulutuksen palautejärjestelmä, yliopistopedagoginen koulutus, kansainvälinen henkilöstöliikkuvuus sekä kansainvälinen opiskelijaliikkuvuus. Kansainvälisen liikkuvuuden kehittämistoimenpiteet valmistuivat kevään seurannan jälkeen. Kehitystyö on edelleen kesken koulutuksen palautejärjestelmän ja yliopistopedagogisen koulutuksen osalta. Koulutuksen palautejärjestelmän kehittämistoimenpiteet on määritelty uudelleen ja projektiin on allokoitu resursseja. Yliopistopedagogisen koulutuksen kehittämistoimenpiteet on myös uudelleen tarkasteltu ja suuri osa toimenpiteistä on aikataulutettu ja sidottu käynnissä olevaan OPS-prosessiin.

3.1.3 Laadunhallinnan tilannekuva

Laatujärjestelmä

Vaikka yliopiston laatujärjestelmä todettiin vuonna 2021 Karvin toteuttamassa laatujärjestelmäauditoinnissa tasolle hyvä, ei laatujärjestelmämme vielä edelleenkään täysin kata yliopiston perustehtävistä yhteiskunnallista vuorovaikutusta, vaikuttamista ja vaikuttavuutta. Yhteiskunnallisen vuorovaikutuksen ja vaikuttavuuden integroiminen kattavammin osaksi laatujärjestelmää on käynnistynyt hitaasti. Suunnitelmat ja kehittämistyö esimerkiksi toimintaa kuvaavien ja tavoitteiden toteutumista seuraavien indikaattoreiden määrittelyn, datan keruun

sekä tavoitteiden toteutumisen seurantamallin osalta eivät näytä edenneen. Myös laatujärjestelmän vahvistamistyö on edennyt hitaasti ja koulutuksen palautejärjestelmä on ollut kehitystyön alla jo useamman vuoden, ja osa säännöllisestä palautesyklin palautetiedosta on jäänyt keräämättä jo muutaman kierroksen verran.

Omistajuuksia ja vastuurooleja ei ole edelleenkään täysin määritelty. Yliopiston laatukäsikirja on ollut kehittämisen alla jo edellisestä 2015 Karvin toteuttamasta laatujärjestelmäauditoinnista lähtien. Laatukäsikirjatyö käynnistettiin uudelleen 2020 toimintakäsikirjana ja uudistuvan toimintakäsikirjan perustana on ollut toiminnan rakenteisuus, kokonaisarkkitehtuuri sekä kyvykkyysajattelu. Toimintakäsikirjatyö siirrettiin pois laadunohjausryhmän ohjauksesta. Toimintakäsikirjasta hyväksyttiin 1.12.2020 osin keskeneräinen toimintarakenteen suppea kirjallinen versio 1.0, ja tavoitteena oli jatkaa projektin tavoitteenasettelun mukaista työtä vuoden 2021 aikana. Toimintakäsikirjatyö eteni hitaasti ja työ keskeytettiin lukuvuoden 2021–2022 aikana.

Tiedolla toimimisen edellytyksiä on vahvistettu viime vuosina ja laatujärjestelmän kyky tuottaa informaatiota johtamisen ja toiminnan kehittämisen tueksi on parantunut. Tiedolla toimimisen kypsyystaso on kuitenkin kokonaisuudessaan vielä matala. Raportoinnin osalta on tähän mennessä pääasiassa saatu systematisoitua vain vuosiraportoinnin kokonaisuus, mutta yksiköt ovat löytäneet tiedontuotannon palvelukanavan ja erillisten tietopyyntöjen määrä on lisääntynyt.

Laadunohjausryhmä nosti vuoden 2021 laadunhallinnan tila -katsauksessa kehittämiskohteeksi kokonaisnäkymän saamisen yliopiston kaikkeen kehittämistoimintaan. Jatkuvaan laadun parantamiseen tähtäävää kehittämistyötä tehdään yliopistossa jatkuvasti, mutta yliopistotasoinen näkymä kehittämistyöhön on edelleen kapea. Tilannenäkymän parantamiseksi sekä kehittämistoiminnan systemaattisemmaksi johtamiseksi yliopisto on hankkinut projektihallintaan ja -johtamiseen Thinking portfolio -järjestelmän, joka otettiin laajempaan yhteisön käyttöön kesällä 2023. Järjestelmän käyttöönotto ei ole edennyt suunnitellussa aikataulussa ja siten yhtenäistä tilannetietoa ei ole vielä saatavilla yliopistolla käynnissä olevista kehittämisprojekteista ja niiden etenemisestä. Laatujärjestelmän tuottama tieto ei ole tältä osin parantunut.

Laatukulttuuri ja toimintatavat

Laadunohjausryhmän näkemyksen mukaan Jyväskylän yliopiston johtamisjärjestelmä tukee hyvin laadunhallintaa ja laadukasta toimintakulttuuria. Organisaation matalat raja-aidat sekä kyky tehdä yhteistyötä yliopiston sisällä tukevat hyvää laatukulttuuria. Yliopistolla nähdään olevan vahva halu kehittää toimintaansa jatkuvan parantamisen hengessä. Vahvuutena on myös halu hyödyntää digitaalisuutta, vaikka heikkoutena edelleen on digitaalisuuden luomien mahdollisuuksien matala hyödyntäminen myös laadunhallinnassa.

Laatukulttuuri voi kuitenkin jäädä arjessa etäiseksi ja laatutyötä ei välttämättä osata mieltää osana päivittäistä toimintaa. Laatutyötä ja toimeenpanoa haastaa myös toimintatapojen epäsystemaattisuus sekä henkilöresursseihin kohdistuvat riskit ja varahenkilöjärjestelmien heikkous.

Laadunvarmistus

Laatukulttuuri on kehittynyt vuosien mittaan ja arvioinnit ovat tulleet yliopistossa tutuiksi toiminnan kehittämisen välineiksi. Sisäisen itsearvioinnin menettelytavalla on jo pitkä historia yliopistolla ja arviointitoimintaan on selkeät prosessit. Vaikka arviointitoiminta on vakiintunut ja tullut osaksi normaalia toimintaa, yliopistolla on puuteellinen kyky hyödyntää arviointipalautetta ja suosituksia systemaattisesti kehittämistyössä. Yliopiston tulisi selkiyttää arviointipalautteen käsittelyprosessia ja systemaattista hyödyntämistä.

Yliopiston laadunhallinta on painottunut viime vuodet laadunvarmistukseen, ja arviointitoiminnan runsauden vuoksi on myös vaarana, että laatutyön kokonaiskuva hämärtyy.

Poikkeamahallinnan toimintatavat ja kokonaisuus ei ole vielä täysin jäsentynyt, vaikka tietoturvan ja tietosuojan puolella on systemaattisia käytänteitä poikkeamahallintaan. Poikkeamahallintaa kehitetään tällä hetkellä erityisesti turvallisuuden osa-alueella, tavoitteena parantaa yhtenäistä tilannetieto.

Yliopiston laatuarviointien perusteella muodostettuja kehittämistoimenpiteiden etenemistä on seurattu kaksi kertaa vuodessa sisäisten tarkastusten kehittämiskohteiden ohella yliopiston sisäisen tarkastajan ylläpitämässä Audit Log -rekisterissä. Yliopiston sisäisen tarkastuksen organisointi uudistettiin syksyn 2023 aikana ja tarkastustoiminta toteutetaan jatkossa yhteistyössä ulkopuolisen toimittajan kanssa. Tässä yhteydessä poistui myös Audit log -seurantamenettely ja uutta sisäistä seurantaprosessia ja -menettelytapaa ei näille kehittämiskohteille ole vielä määritelty.

Laadun parantaminen

Jatkuvan laadun parantamisen näkökulmasta PDCA-sykli ei toimi täysin johdonmukaisesti, ja erityisesti arviointitoiminnan ja kehittämistyön välissä on havaittavissa epäjatkuvuutta. Kehittämistyö arviointipalautteen ja kehittämissuositusten perusteella ei näyttäydy suunnitelmalliselta ja dokumentoidulta. Suositusten mukaista kehittämistyötä on kuitenkin havaittavissa, ja arviointipalautetta on hyödynnetty toiminnan kehittämisessä. Kehittämispalautteen yhteisölliselle käsittelylle sekä arviointipalautteen perustella muodostetavien kehittämistoimenpiteiden muodostamiselle olisi hyvä määritellä systemaattinen menettelytapa.

3.1.4 Laatutyö ja laadunhallinnan kehittäminen 2024

Laatujärjestelmän kehittäminen

Koulutuksen palautejärjestelmän kehittämistyö on projektoitu ja resursoitu uudelleen vuoden 2023 aikana ja koulutuksen palautejärjestelmän kokonaisuudistus on aikataulutettu vuosille 2023–2026. Vuoden aikana otetaan käyttöön uusi opintojaksopalautejärjestelmä, joka mahdollistaa myös vastapalautteen antamisen sekä vastapalautetiedon antamisen seurannan opintojaksokohtaisesti. Vuoden aikana määritellään ja kehitetään opiskelijapalautekokonaisuus kattamaan koko opiskelijan opintopolku orientaatiokyselystä maisterikyselyyn, huomioiden kehittämistyössä valtakunnallisen kandipalautekyselyn sisältö. Kyselykokonaisuudessa tarkastellaan tiedon hyödynnettävyyttä koulutuksen kehittämisen ja johtamisen prosessien ja

tarpeiden näkökulmasta. Kehittämistyössä käynnistetään myös raportoinnin suunnittelu sekä palautteiden käsittelyn toimintamallin rakentaminen.

Laadunohjausryhmä on todennut toimintakäsikirjatyön nimellä toteutetun laatukäsikirjan viivästyneen ja laadintaprojektin keskeytyneen. Yliopistolta on puuttunut voimassa oleva laatukäsikirja jo vuodesta 2017 lähtien, jolloin uuden laatukäsikirjan suunnittelutyötä käynnisteltiin. Toimintakäsikirjan, joka tavoitteena on kuvata mm. ydintehtävien ja tukipalveluiden toimintoja, prosesseja, prosesseissa tuotettuja palveluita sekä toiminnan vastuita, rinnalle on esitetty laadittavaksi laatukäsikirjaa täydentämään toimintakäsikirjaan tulevia sisältöjä. Uuden laatukäsikirjan suunnittelu on käynnistymässä ja laatukäsikirjan sisällöiksi on suunnitteilla mm. laatujärjestelmän kuvaus synkronoituna johtamisjärjestelmään, strategiaohjaukseen ja toiminnan ohjaukseen, kuvaus perustehtävien ja tukipalveluiden laadusta ja laadunhallinnasta sekä koonti Jyväskylän yliopistossa käytettävistä laadunhallinnan menettelytavoista.

Kevään 2024 aikana uudistetaan yliopiston toiminnan suunnittelun ja seurannan prosessia. Tavoitteena on kytkeä yliopiston strategiaohjauksen ja toiminnan ohjauksen mallit yhdeksi kokonaisuudeksi, jossa yliopiston strategia ohjaa yksiköiden toimintasuunnitelmia niin sisällön kuin rakenteen osalta. Uudistusprosessi olisi myös mahdollisuus kytkeä toiminnan ohjauksen prosessiin uusia laadunhallinnan elementtejä ja siten vahvistaa yliopiston laatujärjestelmän kattavuutta.

Tiedolla toimimisen edellytyksiä parannetaan uusilla keskitetysti tuotetuilla raporteilla. Avoimen yliopiston tuottaman koulutuksen Sisu-raportoinnin toteutus valmistuu vuoden 2024 aikana. Yliopiston ja yksiköiden johdolle suunnatusta Tilannekartasta (aik. johdon dashboard) julkaistaan ensimmäinen versio. Yliopiston keskitettyä julkaisuraportointia kehitetään ja tuodaan laajemman käyttäjäjoukon saataville PowerBI-raportointialustan myötä. Julkaisuraportoinnin kehittämisen rinnalla Avoimen tiedon keskus kehittää julkaisujen sisällöllistä raportointia täydentämään edellä mainittuja tilastotietoja.

Laadun suunnittelu ja ohjaus

Vuoden aikana on tavoitteena määritellä ja kuvata laadunhallinnan menettelytavat ja prosessit, erityisesti menettelytapa kehittämistoimenpiteiden määrittelyyn arviointipalautteen perusteella sekä kehittämistoimenpiteiden seurantaprosessi vähintään näiden osalta. Lisäksi määritellään prosessi Jyväskylän yliopiston arviointiohjelman laatimiseksi ja hyväksymiseksi sekä selvitetään mahdollisuus kytkeä hyväksymisprosessi toiminnan ohjauksen vuosisuunnittelun prosessiin.

Yhdenvertaisuus-, tasa-arvo- ja saavutettavuus -kehittämisryhmän tavoitteena on tänä vuonna yhdistää JYU:n saavutettavuussuunnitelma sekä yhdenvertaisuus- ja tasa-arvosuunnitelma yhdeksi kokonaisuudeksi. Samalla nykyisten suunnitelmien toimenpiteiden toteutus arvioidaan sekä asetetaan mitattavissa olevat tavoitteet ja toteuttavat toimenpiteet saavutettavuuden, tasa-arvon ja yhdenvertaisuuden edistämiseksi vuosina 2025–2027.

Uusissa käynnistyvissä Vasara-järjestelmään mallinnettavissa sähköisissä prosesseissa kokeillaan uutta toimintamallia, jossa pyritään tunnistamaan jo suunnitteluvaiheessa prosessiin liittyvät asianhallinnan ja raportoinnin kiinnityskohdat, jotta voitaisiin ennakoida näihin kohdistuvia vaikutuksia.

Vasara-järjestelmään digitalisoidun rekrytointiprosessin automatisoidun raportoinnin kehittämisen yhteydessä luodaan uutta tapaa hyödyntää Power BI:tä yksittäisen järjestelmän raportoinnin alustana. Aiemmin vastaavat automaattisesti päivittyvät raportit on tuotettu yliopiston tietovaraston avulla. Vuoden aikana kuvataan Power BI:n hyödyntämisen yleinen malli. Mallissa kuvataan periaatteet ja yliopiston palvelut Power BI:n hyödyntämiseen huomioiden erityisesti tietoturvan ja tietosuojan näkökulmat ja kokonaisuuden hallittavuuden.

Laadunvarmistus

Vuonna 2024 on käynnissä yksi yliopistotasoinen arviointiprosessi sekä yhden tulevan arviointiprosessin suunnittelu. Lisäksi toteutetaan kaksi yksikkötason akkreditointiprosessien arviointivierailua.

Olympiakomitean toteuttamaan Huippu-urheilijamyönteinen korkeakoulu -auditointiprosessin tulos julkistetaan toukokuussa 2024 Oppilaitosseminaarin yhteydessä. Arviointipalaute ja -suositukset tullaan käsittelemään yhteisöllisesti ja palautteen perusteella laaditaan tarvittavat kehittämistoimenpiteet. Arviointiprosessista vastaa koulutusneuvosto.

Tutkijan uran ja työskentelyedellytysten edistämiseen keskittyvän Human Resources Strategy for Researchers (HRS4R) -prosessin ulkoinen arviointivierailu toteutetaan 2026. Suunnittelu käynnistetään syksyllä vuoden 2025 aikana toteutettavasta prosessiin sisältyvästä itsearvioinnista sekä valmistautumisesta arviointivierailuun. Prosessin ohjauksesta vastaa Osaava, luova ja hyvinvoiva yliopistoyhteisö -kehittämisryhmä.

Jyväskylän yliopiston kauppakorkeakoulun AACSB-akkreditointivierailu toteutetaan 23.–25.3.2024 sekä AMBAn ja BGAn uudelleenakkreditoinnit toteutetaan 2.–3.12.2024.

Yliopiston poikkeamahallinnan kehittäminen jatkuu edelleen. Yliopistoon hankittiin vuoden 2023 aikana riskienhallintajärjestelmä, jonka yhtenä elementtinä on turvallisuushavaintojen ilmoittaminen ja käsittely. Käyttöönoton yhteydessä oli tavoitteena luona turvallisuuspoikkeamille systemaattiset ilmoittamis- ja käsittelytoimintatavat. Järjestelmän toiminnallisuuksien käyttöönotto ja toimintatapojen jalkauttaminen yliopistoyhteisöön on vielä kesken.

Laadun parantaminen

Arviointitoiminnan perusteella määriteltyä kehittämistyötä jatketaan koulutuksen palautejärjestelmän kehittämisen sekä yliopistopedagogisen koulutuksen osalta. Yhteiskunnallisen vuorovaikutuksen ja vaikuttamisen kytkentä laatujärjestelmään vahvistunee strategiaprosessin yhteydessä. Huippu-urheilijamyönteinen korkeakoulu- auditointiprosessista määritellään tarvittavat kehittämistoimenpiteet auditointipalautteen saavuttua.

Human Resources Strategy for Researchers (HRS4R) -prosessiin sisältyvässä toimenpideohjelmassa on edellisen vuonna 2022 tehdyn itsearvioinnin perusteella määriteltynä 13 kehittämistoimenpidettä tutkijan uran ja työskentelyedellytyksien parantamiseksi. Toimenpiteet ovat kytköksissä strategian kehittämisohjelmiin ja edistävät erityisesti Osaava, luova ja hyvinvoiva yliopistoyhteisö -kehittämisohjelman ja tutkimuksen kehittämisohjelman päätavoitteita.

3.2 Riskienhallinta

3.2.1 Riskienhallinta Jyväskylän yliopistossa

Riskienhallinta on tärkeä osa yliopiston toiminnan suunnittelua ja toiminnan prosesseja. Riskienhallinnalla tarkoitetaan niiden epävarmuuksien hallintaa, jotka vaikuttavat asetettujen tavoitteiden saavuttamiseen. Epävarmuudet voivat olla joko mahdollisuuksia tai uhkia tai molempia. Riskienhallinnan keskeisimpänä tavoitteena on varmistaa yliopiston toiminnan tuloksellisuus ja jatkuvuus.

Riskienhallinnan päämääränä on hallita yliopiston kokonaisriskiä, ei ainoastaan yksittäisiä riskitekijöitä. Riskienhallinnalla varmistetaan päätettyjen toiminnallisten ja strategisten tavoitteiden saavuttaminen, lakisääteisten vaatimusten sekä toimielinten ja johdon päätösten noudattaminen ja toteutuminen. Lisäksi riskienhallinta tukee omaisuuden sekä voimavarojen turvaamisessa. Riskienhallinta perustuu tietoon perustuvalle päätöksenteolle ja se on osa yleistä johtamis- ja hallintojärjestelmää. Riskien näkökulma on sisällytetty yliopiston prosesseihin ja päätöksentekoon. Riskienhallinta on osa yliopiston jatkuvaa ja toistuvaa toimintaa, joka integroituu kaikkiin yliopiston suunnittelu- ja toimintaprosesseihin.

3.2.2 Keskeiset tapahtumat edellisen raportin jälkeen

Uusi varmennustoiminnan politiikka ja periaatteet määrittelee varmennustoiminnan tavoitteet, periaatteet, vastuut ja valtuudet hallita riskejä sekä kuvaa riskienhallintaprosessin. Tämä politiikka muodostaa yhdessä muiden yliopiston toimintaohjeiden kanssa kokonaisuuden riskien hallitsemiseksi ja se käsittää Jyväskylän yliopiston, sekä sen alaisten tiedekuntien, erillislaitosten sekä yliopistopalveluiden nykyisen ja tulevan toiminnan sekä toiminnan suunnittelun.

Vuoden 2023 aikana tehtiin investointipäätös teknologian hankinnasta tukemaan turvallisuuden ja riskienhallinnan johtamista yliopistossa. Teknologiaksi valittiin kilpailutuksen kautta Qreform Rego niminen teknologia. Tekninen käyttöönottoprojekti toteutettiin vuoden 2023 aikana. Vuoden 2024 aikana teknologian käyttöönoton tukeminen aloitetaan jokaisessa tiedekunnassa, erillislaitoksessa sekä yliopistopalveluissa osana yksiköiden road show-tilaisuuksia.

Ulkoisen kumppanin toteutukseen siirretty sisäinen tarkastus kytkeytyy riskienhallintaan, ja sisäiset tarkastukset toteutetaan riskiperusteisesti. Vuoden 2023 riskeistä on koottu tilannekuva uuden riskienhallinnan taksonomian mukaisesti ja tätä dataa tullaan hyödyntämään suunniteltaessa kuluvan ja tulevan vuoden sisäisiä tarkastuksia.

Toimintasuunnitelmien yhteydessä toteutettiin kussakin yksikössä kevyt riskitarkastelu. Osa yksiköistä päivitti johdon riskikartoituksen, osa ei. Tämä oli tarkoituksenmukainen toimintatapa, kun samalla olimme uudistamassa riskienhallinta prosessia osana varmennustoiminnan politiikkaa ja periaatetta.

Riskienhallintaan liittyviä pistemäisiä koulutuksia on tarpeen vaatiessa toteutettu yliopistossa. Vuoden 2023 aikana on myös lisätty riskienhallinnan henkilöresursointia.

3.2.3 Riskienhallinnan tilannekuva

Jyväskylän yliopiston toimintaympäristö muuttuu nopeasti ja samoin yliopistoa kohtaavat riskit ja mahdollisuudet lisääntyvät. Riskienhallinnasta tulee jatkuvasti tärkeämpi toiminnan menestystekijä, eikä enää riitä pelkästään omaan toimintaan liittyvien riskien tarkastelu, vaan riskienhallinnan näkökulmaa on tarpeen laajentaa myös oman toiminnan ulkopuolelle.

Yliopiston menestymisen kannalta on yhä tärkeämpää ottaa riskienhallinta osaksi yliopiston jokapäiväistä arkista toimintaa sekä johtamista. Asenteet riskienhallintaa kohtaan ovat muuttuneet hyvään suuntaan, mutta kulttuurin muuttaminen vie vielä aikaa. Jyväskylän yliopistossa on aloitettu järjestelmällinen työ riskien- ja mahdollisuuksienhallinnan kulttuurin kehittämiseksi ja tätä jatketaan läpi kuluvan ja tulevien vuosien. Olennaisinta on saada aikaan toimivia käytäntöjä, jotka ovat osa arjen toimintaa ja johtamista, ei vain pelkkiä muodollisia dokumentteja. Lisäksi tulee huolehtia, että koko henkilökunta tuntee riskienhallinnan periaatteet ja käytännöt. Riskienhallinta ei voi olla yksilösuoritusten varassa, vaan sen on integroiduttava osaksi johtamismalliamme ja arjen toimintaa.

Yliopistotasolla ei suuria muutoksia yliopistotasoisiin riskeihin verrattuna viime vuoteen. Tietoturvaan liittyvien riskien trendi on kasvava ja näiden riskien realisoitumisesta aiheutuneet taloudelliset kustannukset ovat trendiltään myös kasvavia. Myös toiminnan nykymuotoinen, digitaalisuuteen vahvasti nojaava toimintamalli on haavoittuva edellä mainitun uhkan takia. Miten valmiita olemme mukauttamaan toimintaamme, mikäli tietojärjestelmiä, verkkoyhteyksiä tai digitaalista infrastruktuuria ei edellä mainittujen uhkien toteutumisen vuoksi ole käytössä? Muutosjohtamiseen sekä muutoskykyyn liittyvät asiat ovat tulevaisuuteen peilaten entistä tärkeämmässä roolissa yliopiston pidemmän tähtäimen tavoitteiden saavuttamiseen liittyen.

Työn vaarojen arviointiin (työn riskien arviointi) on nyt olemassa tukeva teknologia osaamista auttamaan ja tukemaan yksiköitä työn vaarojen arvioinnissa. Aiemmin emme ole täyttäneet työn vaarojen arviointiin liittyviä vaatimuksia, mutta nyt siihen on olemassa toimintamallit, osaaminen ja teknologia.

3.2.4 Riskienhallinta ja riskienhallinnan kehittäminen 2024

Riskienhallinnan kulttuurin kehittäminen on keskeinen teema, jota toteutetaan jokaisessa yksikössä yksiköiden road show-tilaisuuksien kautta. Näissä tilaisuuksissa tuodaan tutummaksi yksiköiden arkeen varmennustoiminnan politiikkaa, missä yhtenä osa-alueena on riskienhallinta sekä siihen liittyvät vastuut ja toimintamallit. Kulttuurin kehittäminen tarkoittaa sitä, että riskienhallinta on vahvemmin osana yksiköiden arkea ja sen johtamista. Kulttuurin kehittämisessä tärkein asia on johdon sitoutuminen ja esimerkin näyttäminen. Käytännössä tämä tarkoittaa sitä, että toimintamallit ja niitä tukeva teknologia on vietävä yksiköiden sekä yliopiston johtamisjärjestelmään ja arkeen osaksi jokapäiväistä johtamistyötä.

Vuoden 2024 aikana toteutetaan systemaattisesti turvallisuuskävelyitä sekä työn riskien arviointia osana yksiköiden riskienhallinnan ja turvallisuuden kulttuurin kehittämistä. Yksiköiden johtoa tuetaan ja valmennetaan riskienhallinnan prosessin laadukkaampaan toteuttamiseen myös johdon riskikartoituksien kanssa toimintasuunnitelmien (TS) valmistelun yhteydessä.

Rooleja ja vastuita on kuvattu yhtenäisemmällä tasolla yliopistotasoisesti. Tätä roolien ja vastuiden tarkentamista jatketaan yksikkötasoisesti.

Syksyllä TS-prosessin yhteydessä yksiköissä tunnistetut riskit ja niiden elinkaaren hallinta tullaan toteuttamaan Qreform Rego -järjestelmässä. Tässä yhteydessä tullaan hyödyntämään myös uutta riskienhallinnan taksonomiaa osana tunnistettujen riskien ryhmittelyä. Luovumme erillisistä yksikkökohtaisista Excel-tiedostoista ja luomme vahvemmin yhtenäisen yliopistotasoisen tilannekuvan.

Varmennustoiminnan tila raportti 2024 tulee tarkastelemaan vahvemmin riskienhallintaa järjestelmässä olevan informaation kautta. Toimintaa ja johtamista tuetaan ja kehitetään siten, että tiedolla toimimiseen liittyvä informaatio riskienhallintaan löytyy Rego järjestelmästä.

3.3 Turvallisuus

3.3.1 Turvallisuuden hallinta Jyväskylän yliopistossa

Turvallisuuden hallinnalla tarkoitetaan Jyväskylän yliopiston kaikkien toimintojen turvallisuutta. Turvallisuuden hallinnalla voidaan suojata yliopistolle tärkeitä arvoja kuten henkilöitä, tietoa, mainetta, omaisuutta tai ympäristöä niihin kohdistuvilta riskeiltä.

Turvallisuudenhallinnan keskeinen tehtävä on edistää yliopiston kilpailukykyä ja parantaa tuottavuutta. Turvallisuusjohtaminen on osa normaalia organisaation johtamista. Tavoitteena ei ole erillinen turvallisuustoiminto, vaan yliopiston toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden varmistaminen kaikissa tilanteissa, luonnollisena osana organisaation riskienhallinnan kokonaisuutta.

Tavoitteena olisi, että turvallisuudenhallinta olisi osana yliopiston laatujärjestelmää ja tuottaisi yliopistolle, yliopistoyhteisölle sekä yhteistyökumppaneille lisäarvoa. Sen vuoksi turvallisuuden jatkuva kehittäminen on kannattavaa.

Organisaation turvallisuudenhallinnan kentän hahmottamiselle, tarkastelulle ja kehittämiselle luo pohjan Elinkeinoelämän Keskusliiton yritysturvallisuusmalli. Siinä turvallisuusjohtaminen jaetaan yhdeksään eri osa-alueeseen. Nämä osa-alueet ovat toimitila- ja kiinteistöturvallisuus, toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, henkilöstöturvallisuus, pelastusturvallisuus, tietoturvallisuus, väärinkäytösten ja poikkeamien hallinta sekä varautuminen ja kriisinhallinta. Jyväskylän yliopistossa tähän jaotteluun on lisätty myös erillisenä osa-alueena opiskeluturvallisuus. Tätä viitekehystä ja jaottelumallia hyödynnetään myös Jyväskylän yliopiston turvallisuuden tarkastelussa ja kehittämisessä.

Turvallisuuden asiantuntijuudesta ja yliopistotasoisen organisaatioturvallisuuden kehittämisestä vastaavat riskienhallinta- ja turvallisuuspäällikkö, tietoturvapäällikkö, turvallisuusasiantuntija, työsuojelupäällikkö sekä palvelupiste Claviksen henkilöstö.

3.3.2 Keskeiset tapahtumat edellisen raportin jälkeen

Yliopiston turvallisuuden kehittämistä jatkettiin aiempien suunnitelmien pohjalta. Henkilövaihdokset ovat jonkin verran hidastaneet suunnitelmien toteuttamista, mutta kehitystyötä on saatu silti kohtuudella edistettyä. Yliopiston käyttöön hankittu turvallisuuden ja riskienhallinnan Rego-järjestelmän käyttöönotolla tuetaan riskiperustaista turvallisuuden hallintaa ja kehittämistä. Turvallisuuteen liittyvän tiedonkäsittelyn keskittäminen yhteiseen järjestelmään antaa paremman mahdollisuuden turvallisuuteen ja riskeihin liittyvään ilmoittamiseen, arviointiin, viestimiseen, raportointiin ja tilannekuvan muodostamiseen. Järjestelmä on saatu käyttöön, mutta ilmoitusten käsittelyyn liittyvien roolit ja vastuut käydään läpi yliopiston tiedekuntien ja erillislaitosten johdon nimeämien tahojen kanssa, jotta vastuulliset osaisivat käsitellä saapuneita ilmoituksia. Rego-järjestelmää hyödynnetään myös työn riskien

arviointiin sekä turvallisuuskävelyihin, joiden avulla pyrkimyksenä on havaita turvallisuuteen liittyviä riskejä ja ottaa niitä hallintaan.

Alkuvuodesta 2024 otettiin yliopistossa pilotointikäyttöön kriittisen viestinnän ja sisäisen hälyttämisen mobiiliapplikaatio Secapp. Kevään 2024 aikana järjestelmän käyttöön koulutetaan Ylistönrinteellä työskentelevät yliopiston työntekijät, tilapalveluiden henkilöstö sekä yliopiston kriisijohto (laaja johtoryhmä) tukiorganisaatioineen (asiantuntijat). Käyttäjäjoukko kahden vuoden pilotointijaksolla on n. 700 henkilöä. Ensimmäiset käyttökokemukset järjestelmästä Ylistönrinteellä ovat olleet positiivisia ja osoittaneet sen tarpeellisuuden.

Vuonna 2022 aloitettua yliopiston valmius- ja varautumissuunnitelman päivitystyötä jatkettiin keväällä 2023 ja päivitetty versio on vielä viimeisteltävänä, jonka jälkeen se viedään hyväksyttäväksi. Varautumissuunnittelu on yhteiskunnan turvallisuustilan muutosten, häiriötilanteiden ja kriisienhallinnan näkökulmasta merkityksellistä ja vaikuttaa yliopiston kykyyn selvitä tällaisista tilanteista ja hallita niiden vaikutuksia. Yliopistolaki velvoittaa yliopistoja tekemään valmius- ja varautumissuunnittelua ja jatkamaan toimintaansa kaikissa yhteiskunnan turvallisuustiloissa. Tätä ei ole erityisen hyvin huomioitu yliopiston infran tai toiminnan suunnittelussa.

Tapahtumien turvallisuussuunnittelu on osoittautunut osin puutteelliseksi ja sitä on lähdetty korjaamaan turvallisuuden asiantuntijoiden ohjaamana. Etenkin avoimien yleisötapahtumien ja -tilaisuuksien osalta tulkinta kokoontumislain ja pelastuslain vaatimuksien osalta on ollut historiassa virheellistä. Pääsäännön mukaan em. lakien perusteella yli 200 hengen avoimista yleisötilaisuuksista on tehtävä poliisille ilmoitus sekä laadittava yleisötapahtuman pelastussuunnitelma, joka lähetetään pelastusviranomaisten arvioitavaksi. Tällaiset tilaisuudet vaativat useimmiten hankittavaksi järjestyksenvalvontaa sekä nimettäväksi henkilöitä ensiapuvalmiuteen. Asiasta on keskusteltu sekä viranomaisten edustajien että yliopiston tapahtumajärjestäjien kanssa ja sitä kautta tilannetta on saatu parannettua. Myös yliopiston käytössä olevien kiinteistöjen pelastussuunnitelmia on tullut kehittää, jotta tapahtumien turvallisuus- ja pelastussuunnittelu onnistuisi helpommin. Tapahtumien turvallisuussuunnittelu on osa laadukkaiden ja vastuullisten tilaisuuksien järjestämistä.

Viimeisen vuoden aikana kansalaisaktivismi ja mielenilmaisut ovat näkyneet ja puhuttaneet jonkin verran myös yliopistossamme. Yliopiston päärakennuksella tehtiin syksyllä 2023 opiskelijaryhmittymän toimesta useamman vuorokauden kestänyt rakennuksenvaltaus, joka hoitui hyvässä yhteistyössä siihen osallistuneiden opiskelijoiden ja yliopiston johdon välillä. Yliopiston johto päätti sallia tilojen käytön tässä tarkoituksessa ja siihen liittyvät turvallisuusjärjestelyt tehtiin yhdessä tähän osallistuneiden opiskelijoiden ja yliopiston henkilökunnan kanssa. Kansainvälisiin kriiseihin liittyvät mielenilmaukset ovat myös näyttäytyneet jonkin verran yliopistokampuksella, mutta niistä ei toistaiseksi ole aiheutunut suurempia ristiriitoja tai uhkia.

Matemaattis-luonnontieteellisen (MLTK) tiedekunnan toiminnan turvallisuuden kehittäminen on jatkunut edellisvuosista kehittämällä henkilöstön ja muissa suhteissa toimivien koulutusta ja osaamista, erilaisissa poikkeamatilanteissa toimimista, turvallisuusviestintää sekä

turvallisuuteen liittyviä rooleja ja tehtäviä selkiyttämällä. Etenkin Ylistönrinteen kampuksen toiminnan turvallisuus on haastava ja monimutkainen kokonaisuus, joka vaatii erittäin monien ja monipuolisten riskien hallintaa. MLTK:ssa on resursoitu henkilöitä turvallisuuteen tiedekunta- ja laitostasoilla, ja nimetty turvallisuuteen liittyviä toimielimiä. Tällaisia toimielimiä ovat tiedekunta- ja laitos- sekä Nanotiedekeskustasoiset turvallisuus- ja kriisiryhmät. Häiriötilanteiden hallintaa varten on myös nimetty henkilöitä, jotka vastaavat niiden johtamisesta, viestimisestä ja evakuointitoimista. MLTK:ssa on myös ollut käytössä vaaratilanteista ilmoittamiseen tarkoitettu lomakejärjestelmä, jolla tietoa poikkeamatapahtumista on kerätty ja ohjattu päätöksentekijöille. Nämä ovat johtaneet kehittämistoimiin, kuten esimerkiksi yliopistossa tehtävien tulitöiden turvallisuuden parantamiseen.

Opiskelijoiden mielenterveyteen liittyviä haasteellisia tilanteita on ollut aiempaan nähden kohtalaisen runsaasti. Mielenterveysongelmat ovat näyttäytyneet hyvin poikkeavana, muissa huolta tai jopa pelkoa herättävänä käytöksenä. Mielen ongelmat ovat näyttäytyneet myös sekavien, asiattomien tai uhkaavien sähköpostien tai kirjeiden lähettämisinä. Haastavimpien tapausten kohdalla turvallisuuden asiantuntijat ovat aktiivisesti viestineet tilanteesta viranomaisten kanssa ja ohjanneet huolta heille. Tällaisiin tilanteisiin puuttumisoikeudet avoimissa ja julkisissa tiloissa kuuluu pääosin viranomaisille. Paikallisessa poliisissa on nimetty huolta herättävien henkilöiden yhdyshenkilöitä, joiden kanssa tällaisista tapauksista on viestitty aktiivisesti. Heiltä on myös saanut hyviä neuvoja, ja he ovat tarpeen mukaan ohjanneet huolta myös sosiaali- ja terveysviranomaisten suuntaan.

Viranomaisten kyky puuttua mielenterveyden ongelmiin on varsin rajallista, jollei henkilöllä itsellään ole halukkuutta hakeutua hoitoon. Myös yliopiston kyky taata yliopistolain mukainen turvallinen opiskeluympäristö ja työturvallisuuslain mukainen turvallinen työympäristö on nykyisillä puitteilla erittäin haastavaa tällaisissa tapauksissa. Yliopistolain mukaisten järjestyssääntöjen asettaminen saattaa hieman auttaa tilannetta, mutta silti etenkin ennakoivat puuttumiskeinot tulevat olemaan heikot. Vaikka esim. opiskelijalle antaisi määräaikaisen erottamispäätöksen opinnoistaan uhkaavan tai vaarallisen käytöksen vuoksi, se ei nykylainsäädännön perusteella estä hänen saapumistaan yliopistokampukselle ja liikkumistaan yliopiston avoimissa, julkisissa tiloissa. Hän tai kuka tahansa muukin voi halutessaan osallistua jopa luennoille, jollei perustellusta syystä yleisön pääsyä luentoa seuraamaan rajoiteta.

3.3.3 Turvallisuuden tilannekuva

Yliopistokampukset ovat yleisesti turvallisia paikkoja opiskeluun, työskentelyyn tai muuhun asiointiin. Rikoksia ja vaaratilanteita tulee asiantuntijoiden tietoon toiminnan ja yhteisön kokoon nähden melko vähäisissä määrin. Toiminnan avoimuus ja julkisuus luovat kuitenkin haavoittuvuuden, joka mahdollistaa turvallisuutta vaarantavien tekojen toteuttamisen. Toiminnan avoimuutta ja sen mahdollista rajoittamista tulisikin tarkastella kriittisesti. Lainsäädäntö ei vastaa tähän liittyviä tarpeita esim. erilaisiin häiriöihin ja haastavaan käytökseen puuttumisen näkökulmasta.

Yliopistoyhteisön osalta turvallisuuskulttuuri on yleisesti yhä alhaisella, mutta kehittyvällä tasolla. Turvallisuuteen liittyviä havaintoja tulee asiantuntijoiden tietoon yhteisön kokoon nähden kohtalaisen vähän, eikä turvallisuutta kovin hyvin tunnisteta jokapäiväiseksi, huomioitavaksi asiaksi. Turvallisuus koetaan akateemisessa yhteisössä myös usein rajoittavaksi tekijäksi tai sellaiseksi asiaksi, josta vastuut kuuluvat muille. Sen vuoksi turvallisuuteen liittyviä vastuita, rooleja ja tehtäviä onkin pyritty selkiyttämään. Tämä työ on vielä kesken, mutta sitä pyritään aktiivisesti edistämään asiantuntijoiden toimesta.

MLTK:n osalta on otettu merkittäviä edistysaskeleita, jotta turvallisuutta ja riskejä saataisiin aiempaa paremmin hallintaan. Turvallisuuskoulutusjärjestelmän, erilaisten toimintaohjeiden ja tarkempien vastuiden sekä roolien määrittämisen myötä mahdollisuus estää ennalta vaaratilanteiden ja vahinkojen syntyminen on entistä parempaa. Kehitettävää ja haltuun otettavaa asiaa on kuitenkin edelleen runsaasti. MLTK:n kanssa tehtävästä turvallisuuden kehittämistyöstä on saatavissa hyviä oppeja ja askelmerkkejä myös yliopiston muihin yksiköihin sekä laajemmin koko yliopistoon.

Turvallisuuden kehittämisessä merkittävänä asiana on ollut yhteistyö eri toimijoiden kanssa. Tiivistä yhteistyötä tehdään kiinteistönomistaja SYK:n, Keski-Suomen oppilaitosten ja viranomaisten sekä valtakunnallisella tasolla eri korkeakoulujen kanssa. Myös Opetus- ja kulttuuriministeriö on järjestänyt korkeakoulujen turvallisuusvastaaville suunnattuja tapaamisia, joissa on käyty läpi korkeakoulujen turvallisuuteen ja varautumiseen liittyviä asioita.

3.3.4 Turvallisuus ja turvallisuuden kehittäminen 2024

Turvallisuuden kehittäminen jatkuu erityisesti edistämällä turvallisuushavaintojärjestelmän (Rego) käyttöönottoa ja markkinointia yliopistoyhteisössä. Havainnot ohjataan käsiteltäviksi varmennustoiminnan politiikan mukaisesti tiedekuntien, erillislaitosten, laitosten ja yliopistopalveluiden vastuiden mukaisesti ja käsittelyä tuetaan ja valvotaan turvallisuuden asiantuntijoiden toimesta. Samalla vastuulliset opettelevat käsittelemään ja arvioimaan havaintoja riskeinä sekä suunnittelemaan ja asettamaan niiden hallitsemiseen toimenpiteitä.

Turvallisuuskulttuurin kehittämistä tuetaan myös turvallisuuskävely -toimintatapaa jalkauttamalla. Keväällä 2024 aloitetussa varmennustoiminnan road show:ssa mm. opastetaan ja harjoitellaan turvallisuuskävelyn toteuttamista ja siinä tehtyjen riskien kirjaamista ja käsittelyä. Turvallisuuskävelyt ovat tehokas tapa saada ihmiset havainnoimaan ja kiinnittämään huomiota erilaisiin turvallisuuteen liittyviin asioihin. Rego-tietojärjestelmämme tarjoaa tälle toiminnalle hyvän alustan.

Kriittisen viestinnän ja sisäisen hälyttämisen järjestelmä Secappin pilotointikäyttö jatkuu ja sen eri ominaisuuksia on tarkoitus ottaa vaiheittain laajemmin käyttöön, kunhan käyttäjät saadaan koulutettua ensin perustoiminnallisuuksiin. Secappin käyttöä, sen tarpeen ja erilaisten käyttömahdollisuuksien tarvetta on tarkoitus arvioida aktiivisesti valitun pilotointijakson aikana. Aiempi tekstiviestipohjainen hälytysjärjestelmä testattiin maaliskuussa, ja havaintona oli, että massatekstiviestit eivät saavuttaneet opiskelijoita, mutta henkilöstölle järjestelmä toimi. Jatkoon tullaan kehittämään ratkaisu Secapp ja MyJYU integraatiolla.

MLTK:ssa otetaan keväällä 2024 käyttöön yliopiston omaan Vasara-järjestelmän kautta toteutettava turvallisuuskoulutus. Turvallisuuskoulutusta on tarkoitus antaa kaikille

työntekijöille ja niille opiskelijoille, jotka työskentelevät tiedekunnassa. Turvallisuuskoulutusten sisällöt räätälöidään työtehtävistä ja niihin liittyvistä riskeistä riippuen. Koulutukset voivat liittyä esim. yleiseen toiminnan turvallisuuteen tiedekunta- tai laitostasolla, erilaiseen laboratoriotyöskentelyyn, tiettyihin toimintoihin, tiloihin tai koneiden, laitteiden, ajoneuvojen tai kulkuneuvojen käyttöön. Kouluttamista ohjataan Vasara-työnkulkujärjestelmän kautta ja eri muotoisten koulutusten sisältöjä luodaan parhaillaan.

Turvallisuuden hallinnan erilaisten tarkempien vastuiden, roolien ja kuvaamistyötä on tarkoitus jatkaa jo aiemmin tehdystä. Jotta näissä asioissa on mahdollista onnistua ja kehittyä, on kussakin tehtävässä ja roolissa toimivan tiedettävä omat vastuunsa ja tehtävänsä. Tämä auttaa vastuullisia myös tarvittavien resurssien ja toimijoiden nimeämistä. Kaikkea ei varmasti saada kerralla haltuun ja kuntoon, mutta aihekokonaisuus tai osa kerrallaan pääsemme kohti turvallisempaa ja laadukkaampaa toimintaa.

Myös yliopistotasolla turvallisuuden kouluttamista on pyrkimyksenä kehittää. Poikkeamatilanteissa toimimista kehitetään myös harjoittelemalla erilaisissa häiriö- ja uhkatilanteissa toimimista, kuten esim. palohälytyksissä, sähkökatkoissa tai henkilöuhkatilanteissa.

Aktiivista yhteistyötä muiden toimijoiden kanssa jatketaan. Kehittämisalueet muissakin korkeakouluissa ovat hyvin samanlaisia, joten intressi toimia ja kehittää yhdessä näitä asioita on kohtalaisen suuri. Viranomaisyhteistyö on myös keskeistä yhteisen tilannekuvan muodostamiseksi ja erilaisten uhkien ja vaarojen torjumiseksi.

3.4 Työsuojelu

3.4.1 Työsuojelu Jyväskylän yliopistossa

Työturvallisuus tarkoittaa kunnossa olevia fyysisiä, psyykkisiä ja sosiaalisia työoloja. Työsuojelun avulla varmistamme työturvallisuuden eli terveyden ja turvallisuuden työssä. Työsuojelu on osa johtamista ja esihenkilötyötä sekä työnantajan ja työntekijöiden välistä yhteistoimintaa, jolla huolehditaan siitä, että työtä on turvallista ja terveellistä tehdä.

Jyväskylän yliopiston työsuojelun tavoitteena on kehittää työympäristöä ja työolosuhteita työntekijöiden työkyvyn turvaamiseksi ja ylläpitämiseksi. Lisäksi sen tarkoituksena on tunnistaa ja ennalta ehkäistä työstä ja työympäristöstä johtuvia työntekijöiden fyysiseen ja henkiseen terveyteen kohdistuvia haittoja ja vaaroja sekä torjua vaaratilanteita, työtapaturmia ja ammattitauteja. Työn vaarojen ja haittojen arviointi (työn riskien arviointi) luo perustan työturvallisuuden ylläpidolle ja parantamiselle.

Työsuojelun toimintaohjelma on työnantajan lakisääteinen työn turvallisuutta ja terveyttä edistävä ohjelma ja se sisältää työsuojelun kehittämistoimenpiteet.

Yliopistotasoisesta työsuojelun yhteistoiminnasta ja työsuojelun yhteistoiminta-asioiden käsittelystä (edustuksellinen työsuojelu) vastaa työsuojeluorganisaatio, jonka muodostavat lakisääteinen työsuojelutoimikunta, kaksi työsuojeluvaltuutettua varavaltuutettuineen, työsuojelun yhdyshenkilö Kokkolassa ja työsuojelupäällikkö. Työsuojelutoimikunta koostuu työnantajan edustajista (3 hlöä) ja ammattijärjestöjen valitsemista edustajista (9 hlöä). Yliopistossa toimiva koordinaatioryhmä ja työsuojelutoimikunta tarkastelevat työturvallisuuden ja työsuojelun tilannekuvaa säännöllisesti.

3.4.2 Keskeiset tapahtumat edellisen raportin jälkeen

Työturvallisuuden periaatteet on määritelty osana varmennustoiminnan politiikkaa ja periaatteita. Periaatteet rakentuvat seuraavista:

- hyvästä työn ja työympäristön suunnittelusta, joka toteutetaan siten, että haitallista kuormitusta ei synny
- työn vaarojen ja haittojen tunnistamisesta, niiden poistamisesta ja vähentämisestä ja tarvittavien toimenpiteiden toteuttamisesta vaarojen vähentämiseksi
- työympäristön ja työyhteisön toiminnan tarkkailusta, seuraamisesta ja valvonnasta
- turvalliseen työskentelyyn ohjaamisesta ja opastamisesta - sujuva työ onnistuu hyvän osaamisen ja riittävien resurssien avulla
- yhteistyössä toimimisesta ja tiedottamisesta ja viestinnästä.

Työsuojelun toimintaohjelman toimenpiteet koostuivat pääosin sisäisen tarkastuksen toteuttaman vahinkoriskien arvioinnin mukaisista toimenpiteistä: työturvallisuuden vastuiden määrittelystä ja sisällyttämisestä yliopiston ohjeistukseen sekä perehdyttämisestä niihin, työn riskien arviointiprosessin luomisesta ja käyttöönotosta sekä työsuojelutarkastusten ja työpaikkaselvitysten kehittämistoimien toteutumisen varmistamisesta. Lisäksi toimenpiteitä olivat työsuojeluun liittyvien toimintatapojen esittely työsuojeluorganisaatiolle ja luottamusmiehille, työturvallisuuteen liittyvien pätevyyksien hallinta sekä työssä käytettävien

laitteiden riskien arviointi ja kehittäminen. Toimenpiteet ovat pääosin toteutuneet. Työsuojelutoimikunta on seurannut toimenpiteiden toteutumista sekä työsuojelun tilaa helmikuun 2024 kokouksessaan esittelyn ja keskustelun pohjalta sekä päivittänyt työsuojelun toimintaohjelman vuosittaisia toimenpiteitä. Osana varmennustoiminnan politiikkaa ja periaatteita on määritelty myös työturvallisuutta ja -suojelua koskevia vastuita (linjaorganisaatiossa toiminnasta ja sen suunnittelusta vastuussa olevat, ja joilla on päätäntävaltaa ja käytössään resursseja; jokaisella yliopistoyhteisön jäsenellä oma vastuunsa). Työsuojelun vastuita on jo aiemmin tarkennettu työsuojelun toimintaohjelmassa (työnantajan edustajina toimivat kukin oman asemansa edellyttämässä laajuudessa: lähijohtaja tiiminsä ja yksikön johtaja koko yksikön osalta). Näihin vastuisiin on alettu perehdyttää yksikön johtoa osana varmennustoiminnan road show-tilaisuuksien valmistelua.

HR toteutti työsuojeluosaamisen toimintatapojen esittelyn työsuojelu- ja luottamusmiesorganisaatiolle elokuussa 2023. Työn riskien arvioinnin toimintatapa valmisteltiin ja käsiteltiin työsuojelun yhteistoiminnassa työsuojelutoimikunnassa keväällä 2023. Työsuojelupäällikkö on valmistellut henkilöstölle kohdennetun työturvallisuussivuston (julkaisu maaliskuu 2024). Yliopistoon hankittiin riskienhallintaa ja poikkeamailmoittamista varten Rego-järjestelmä, jota hyödynnetään myös työturvallisuuteen liittyvissä prosesseissa. Turvallisuushavainnot (läheltä piti-tilanteet, vaaratilanteet, myös positiiviset havainnot turvallisuudesta) ilmoitetaan ja käsitellään jatkossa järjestelmässä. Turvallisuushavaintoja voivat Regossa ilmoittaa kaikki havaintoja tekevät (henkilöstö, opiskelijat, vierailijat, apurahatutkijat). Työturvallisuuteen liittyvät yliopistotasoiset pätevyydet on määritelty ja maaliskuussa 2024 otetaan käyttöön Rego-järjestelmän pätevyyksienhallintaosio, johon kirjataan työturvallisuuden osalta henkilöstön voimassa olevat pätevyydet. Työsuojelutarkastusten ja työpaikkaselvitysten toimenpiteet käsitellään ja niiden edistymistä seurataan Rego-järjestelmässä. Työsuojelun toimintaohjelman toimenpiteistä jäi toteutumatta työkoneiden ja -laitteiden riskien arviointi ja tämä kytketään yksikön toteuttamaan työn riskien arviointeihin.

Työterveyshuollon toteuttamat yksikkökohtaiset työpaikkaselvitykset jatkoivat työn ja työolosuhteiden terveellisyyttä koskevan tiedon ja toimenpide-ehdotusten tuottamista. Vuonna 2023 toteutettiin 15 työpaikkaselvitystä (Avoin yliopisto, HYTK, MLTK, yliopistopalvelut ml. yliopistopaino) ja vuonna 2022 toteutettujen työpaikkaselvitysten seurantoja tehtiin 10 yksikössä (MOVI, KTL, YOP siivoojat ja vahtimestarit, LTK ja Vuokatti, OSC/kirjasto ja psykologian laitos. Työterveyshuolto tunnisti työpaikkaselvityksissä 137 riskiä, joista 9 merkittävää, 99 kohtuullista ja 29 vähäistä sekä 129 psykososiaalista voimavaratekijää. Koko yliopiston henkilöstöä koskeva valtakunnallinen yliopistojen työhyvinvointikysely toteutettiin vuonna 2023. Työsuojeluviranomainen ei tehnyt yliopistolla yhtään työsuojelutarkastusta vuonna 2023. Fysiikan laitoksella ja yliopistopalveluissa pilotoitiin Työterveyslaitoksen Työturvallisuuden johtaminen-koulutusta.

Matemaattis-luonnontieteellisessä tiedekunnassa (MLTK) on jatkettu vahvaa työturvallisuuden kehittämistä: turvallisuusohjeita on päivitetty ja luotu ja turvallisuuskoulutusprosessi on kehitetty. Turvallisuus on nostettu pysyväksi teemaksi laitoskokouksissa. MLTK osallistuu sekä Rego-riskienhallintajärjestelmän (työn riskien arviointi, turvallisuushavainnot) että kriittisen viestinnän ja hälyttämisen Secapp-sovelluksen käyttöönottoon. Ylistönrinteellä on toteutettu rakennuksittain (Ambiotica, NSC, fysiikan laitosrakennus) poistumisharjoituksia, joita jatketaan vuonna 2024. MLTK ja liikuntatieteellinen tiedekunta (LTK) osallistuivat

työturvallisuuspätevyyksien määrittelyyn ja pätevyysmatriisien luomiseen osana Rego-pätevyyksienhallintaosion käyttöönottoa.

Yliopistossa tuettiin yliopistoyhteisön jäsenten hyvinvointia monipuolisella hyvinvointi- ja työterveyspalveluiden tarjonnalla ja kannustamalla hyvinvoinnista huolehtimiseen. Lakisääteisen työterveyshuollon lisäksi käytössä on sairaanhoitopalvelut. Yliopistossa työskentelevien fyysistä hyvinvointia tuettiin sähköisellä taukoliikuntasovelluksella (BreakPro), ohjatuilla pienryhmävalmennuksilla sekä uMoven (korkeakoululiikunta) liikuntapalveluilla. Mielen hyvinvoinnin ja stressinhallinnan tukena tarjottiin mindfulness-kursseja, henkilöstön kompassi ja Auntie-palveluja, ajanhallinnan osaamista sekä hyvinvointiwebinaareja mm. aivojen hyvinvoinnista ja keskeytysten hallinnasta. Lähijohtajille tarjottiin hyvinvoinnin johtamisosaamista (Työterveyslaitoksen Työhyvinvoinnin johtaminen, vastuullisen työkäyttäytymisen toimintamallin vaaliminen-työpajat, työyhteisön hyvien tapojen käsittely tiimin kanssa) sekä tukea oman hyvinvoinnin ylläpitoon (palautuminen, stressinhallinta). Valmentavaa työotetta juurrutettiin yliopistossa mm. kouluttamalla yliopistossa sisäisiä coacheja ja mahdollistamalla jokaiselle yliopistolaiselle mahdollisuus coachingiin osallistumiseen.

Vuonna 2023 sattui henkilöstölle 60 ja opiskelijoille 16 työtapaturmaa. Työntekijöiden työtapaturmien määrä jatkoi kasvuaan (+9). Sisäilmaan liittyvän väistösuosituksen on menneen vuoden aikana saanut 3 henkilöä. Syksyllä 2022 ilmeni Normaalikoulun alakoululla kuitupäästöistä aiheutunut sisäilmaongelma, johon liittyvät korjaukset tehtiin ja kuitupäästöt mittaustulosten perusteella loppuivat. Oireilut alkoivat kuitenkin uudestaan vuoden 2023 lopulla, ja uusintamittausten perusteella todettiin toimenpiderajan ylittäviä kuitumääriä osan tutkittujen tilojen osalta. Tilanteen selvittämiseksi on perustettu SYK:n sisäympäristötoimintamallin mukainen projektiryhmä. Henkilöstöä muistutettiin savuttomuudesta ja tuoksuttomuudesta Tulethan tuoksutta-tarrojen avulla. Yliopisto kustantaa sairauskuluvakuutuksen apurahatutkijoille ja järjestää työterveyshuollon tuntiopettajille kriteereiden täyttyessä (kriteerit kuvattu Unossa Apurahatutkijan oppaassa ja Työterveyshuollon sivuilla).

3.4.3 Työsuojelun tilannekuva

Työturvallisuuskulttuurissa on nähtävissä hyvää kehittymistä ja useita toimenpiteitä on toteutettu vuoden 2023 aikana, kuten edellisessä luvussa kuvattiin. Työn riskien arviointiin on määritelty yliopiston systemaattinen toimintamalli ja prosessi, jota tukee Rego-järjestelmän sähköiset työkalut. Tunnistettujen vaarojen poistaminen tai vähentäminen riippuu myös taloudellisista resursseista.

Työturvallisuuden hallintaa tukee määritellyt työturvallisuuden periaatteet, tarkennetut työsuojelun vastuut, määritelty työn riskien arvioinnin toimintamalli, osassa yksiköitä olevat työturvallisuutta edistäviä rakenteita (työturvallisuus osana työtehtäviä, työturvallisuutta, myös henkistä työturvallisuutta edistävät ryhmät) sekä sähköinen systemaattisen toimintatavan mahdollistava työkalu työn riskien arviointiin, turvallisuushavaintojen ilmoittamiseen ja seurantaan ja työturvallisuuden pätevyyksien hallintaan. Työturvallisuuden perehdytystä on kehitetty ja tuotettu.

Työn riskien arvioinnin toimintatapa esitellään vuonna 2024 osana varmennustoiminnan roadshow-tilaisuuksia. Työsuojelun mittaristo on edelleen pääosin reagoivaa ja osoittaa sekä

hyvää että heikompaa kehittymistä. Mittaristo koostuu työhyvinvointikyselyn tuloksista, vakuutusyhtiön työsuojelutilastoista, työterveyden poissaolotilastoista sekä työpaikkaselvitysten tuloksista.

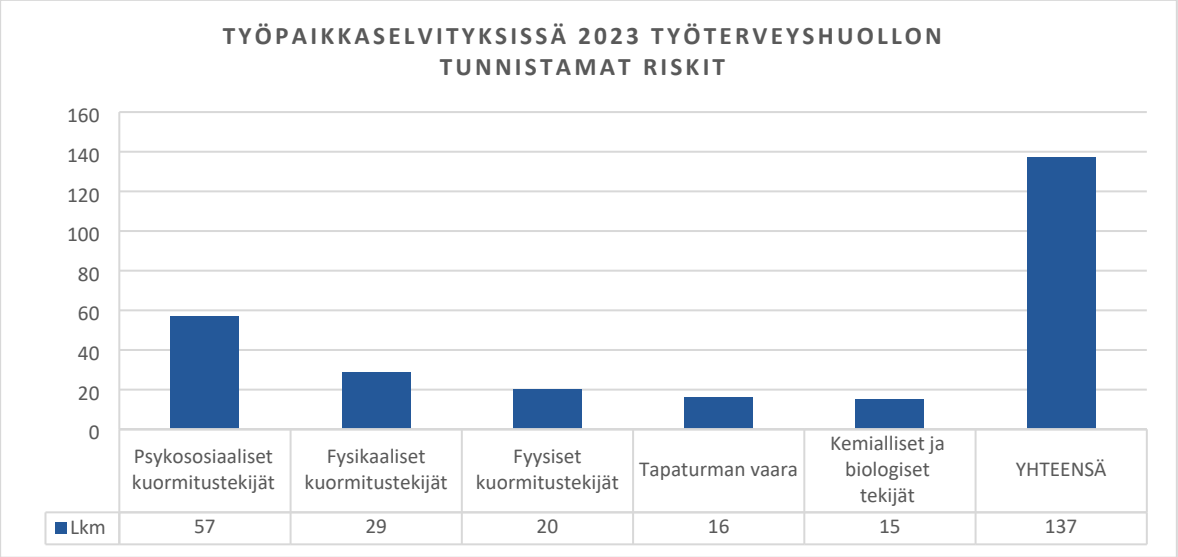
Läheltä piti-tilanteiden ilmoittaminen on yksi työsuojelun ennakoivista mittareista ja tämä toimintatapa on vakiintunut MLTK:ssa. Läheltä piti-tilanteita ja turvallisuushavaintoja kerätään MLTK:ssa ja tilapalveluiden kautta. Vuonna 2023 tilastoitiin 34 turvallisuushavaintoa. Turvallisuushavainnoista nähdään, että läheltä piti-tilanteita sattuu laboratoriotyössä (kemikaalit), ilmanvaihdossa on puutteita (ilmanvaihdon huolto, riittämätön ilmanvaihto vanhemmissa rakennuksissa) sekä ulkoalueiden liukkaus aiheutti vaaratilanteita. Ilmanvaihdon katkeaminen aiheuttaa merkittävää vaaraa laboratoriotyöskentelyssä (kemikaalien vapautuminen hengitysilmaan) silloin kun siihen ei voida varautua, ja valitettavasti tällaisia tilanteita on sattunut.

Työsuojelutoimikunnan SWOT (vahvuudet, heikkoudet, mahdollisuudet, uhat)-analyysin mukaan muutostilanteet tuottavat epävarmuutta yliopistoyhteisössä ja monimuotoisuuden ja joustavuuden säilyttäminen kampuksella sekä opiskelijoiden että henkilöstön näkökulmasta on tärkeää. Yliopistolaiset ovat hyvin palanneet ainutlaatuiselle kampusalueelle. Kuitenkin yhteisöllisyyden rakentuminen hybridityössä edellyttää toimia. Yliopistossa vallitsee hyvä tahtotila työturvallisuuden parantamiseen. Työntekijöiden työturvallisuuden koulutus ja perehdytys on edelleen puutteellista. Työsuojelusta vastuussa olevien edellytyksiin (aika, osaaminen) hoitaa tehtäviään on edelleen kiinnitettävä huomiota. Esihenkilöiden vastuut näyttäytyvät lisääntyneinä ja esihenkilöiden kuormittuminen on riskinä. Työn riskien arvioinnin tekeminen edellyttää ajankäytönresursseja myös muilta kuin esihenkilöiltä, joten varautuminen työn riskien arviointiin osallistumiseen on huomioitava työn suunnittelussa. Rego-työkalua ei voida vielä käyttää täysipainoisesti, sillä henkilöstön tiedot eivät siirry kaikilta osin oikein Regoon. Työsuojelu- ja työturvallisuuskulttuuria vahvistaisi se, että yliopiston muutostilanteissa työsuojelu ja työturvallisuus nähtäisiin teemoina, joita tarkastellaan toimintoja, työympäristöä, tietojärjestelmiä ja hankintoja suunniteltaessa, sillä työturvallisuuteen liittyvät seikat ovat helpointa ja kustannustehokkainta toteuttaa suunnitteluvaiheessa. Tärkeää on myös pystyä keskustelemaan avoimesti ja argumentoiden vaikeista asioista ja konflikteista.

Valtakunnallisen työhyvinvointikyselyn tulokset kuvaavat keskiarvoista positiivista kehittymistä psykososiaalisen työturvallisuuden osalta. Samoin työpaikkaselvitysten tuloksissa on nähtävissä suuri määrä (129) psykososiaalisia voimavaratekijöitä, jotka tasapainottavat työstä aiheutuvia psykososiaalisia kuormitustekijöitä. Sekä työhyvinvointikysely että vuonna 2023 toteutetut työpaikkaselvitykset osoittavat, että esihenkilötyö koetaan työtä tukevaksi.

Yhteistyö työterveyshuollon kanssa toimii ja työpaikkaselvitykset tuottavat tietoa työolosuhteiden ja työympäristön terveydellisistä riskeistä. Työterveyshuolto jakaa tunnistamansa riskit vähäisiin (29 kpl), kohtuullisiin (99 kpl) ja merkittäviin (9 kpl). Näitä riskejä työterveyshuolto tunnisti 137 vuonna 2023 toteutetuissa työpaikkaselvityksissä. Merkittävät riskit liittyivät altistumisiin syöpävaarallisille kemikaaleille ja bakteereille ja viruksille, erityiseen tapaturman vaaraan, epäasiallisen kohtelun kokemuksiin ja epäsopivaan lämpötilaan. Kemikaali-, bakteeri- ja virusriskiin on jo varauduttu ja suojaustoimet hallussa.

Tunnistetuista riskeistä suurin osa (42 %, 57 kpl) liittyy psykososiaalisiin kuormitustekijöihin ja toiseksi eniten fysikaalisiin kuormitustekijöihin (21 %). Kuva 1.



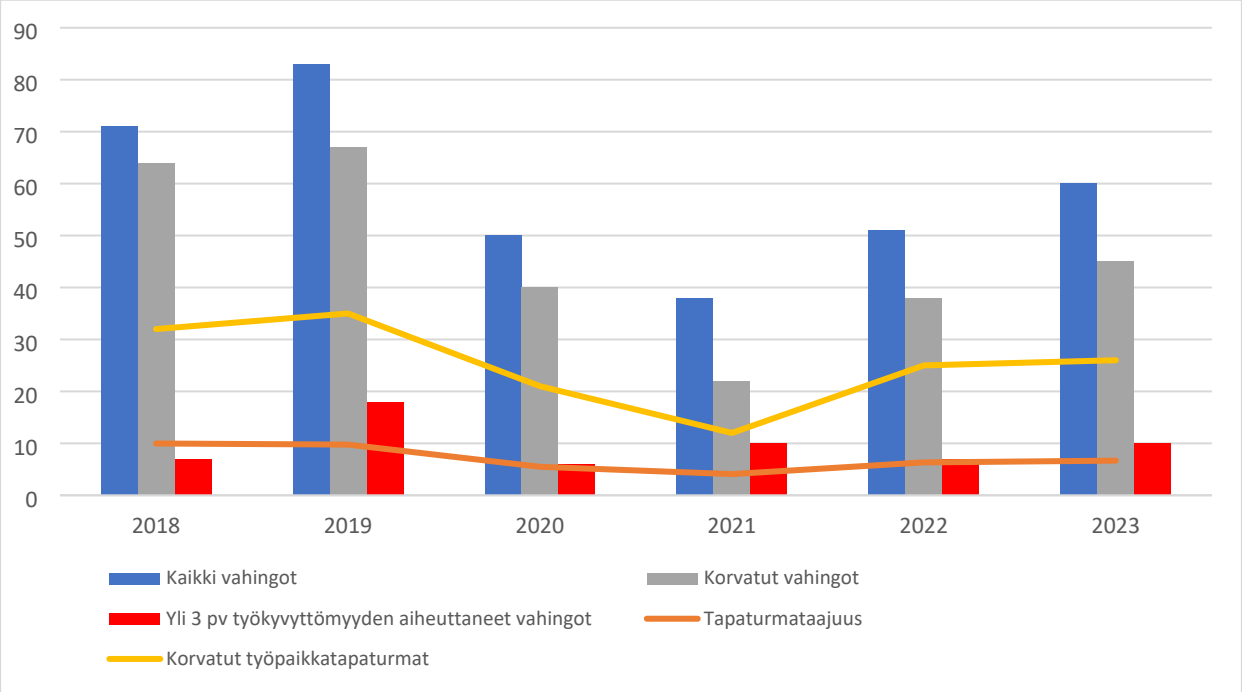
Kuvio 1. Työterveyshuollon vuoden 2023 työpaikkaselvityksissä tunnistamat riskit.

Psykososiaaliset kuormitus- ja voimavaratekijät työpaikkaselvityksissä säilyvät pääosin samoina vuodesta ja yksiköstä toiseen: työtehtävät ovat mielekkäitä, omaa osaamista voi hyödyntää työssään, yhteistyö on toimivaa, omaan työhön voi vaikuttaa ja työn sisällöt ovat mielenkiintoisa. Esihenkilötyö kuvautuu yhtenä useimmin esiintyvästä voimavaratekijöistä ensimmäistä kertaa vuoden 2023 työpaikkaselvityksissä. Psykososiaalisia kuormitustekijöitä ovat työsuhteen jatkuvuus, keskeytykset, tiedon jakaminen, tietojärjestelmät, suuri työmäärä- ja tahti sekä työn organisointi.

Työolosuhteissa (fysikaaliset kuormitustekijät) kuormittaa eniten epäsopiva lämpötila, haittaava ääniympäristö, puutteellinen ilmanvaihto ja huono hengitysilma – erityisesti vanhemmissa rakennuksissa. Tilanne sisäilman suhteen näyttäytyy muutoin rauhallisena. Normaalikoulun alakoulun kuitupäästöt ilmaantuivat uudelleen vuoden 2023 lopulla, ja helmikuussa 2024 aloitettiin kiinteistönomistajan sisäympäristötoimintamallin mukainen toiminta ja ratkaisua haetaan uusilla mittauksilla ja selvityksillä. Fyysisistä kuormitustekijöistä suurin on niska-hartiaseudun kuormittuminen: näyttöpäätetyössä tauotus unohtuu ja etätyössä on usein huonompi fyysinen ergonomia kuin työpaikalla, jossa pääsääntöisesti fyysinen ergonomia on hyvin hoidettu. Kemiallisia ja biologisia kuormitustekijöitä esiintyy erityisesti matemaattis-luonnontieteellisessä tiedekunnassa. Työpaikkaselvityksissä on tunnistettu työn terveellisyyteen liittyvät altisteet hyvin. Suurimmassa osassa yliopiston yksiköitä on vähäinen tapaturmariski ja erityinen/ilmeinen tapaturmariski on laboratorio- ja kenttätyöskentelyssä.

Opiskelijat ovat vakuutettuja opiskelutapaturmalain mukaisesti opetussuunnitelmaan kuuluvassa käytännön työssä ja käytännön harjoittelussa, sekä matkalla käytännön työhön tai harjoitteluun. Opiskelijoille tapahtuneet vahingot sattuvat käytännön opetuksessa, kuten liikuntatieteellisessä tiedekunnassa käytännön liikuntalajeja opiskellessa tai matemaattis-luonnontieteellisessä tiedekunnassa laboratoriotyöskentelyssä. Vuonna 2023 opiskelijat ilmoittivat 16 vahingosta, joten vahingot laskivat yhdellä vuoteen 2022 verrattuna. Vakuutusyhtiö katsoi 11 vahinkoa korvattavaksi. Vahinkojen vammat ovat samoja kuin henkilöstöllä (venähdykset, sijoiltaanmenot, luunmurtumat).

Työntekijöiden työtapaturmien määrä jatkaa nousuaan (+9). Työssä tapahtuneiden tapaturmien määrä on kuitenkin laskenut ja asunnon ja työpaikan välisellä matkalla tapahtuneiden tapaturmien määrä on kasvanut ja muodostaa 42 % kaikista vakuutusyhtiölle ilmoitetuista vahingoista. Yliopistolaisten paluu koronavuosien jälkeen lähityöhön kampuksella todennäköisesti on osasyy asunnon ja työpaikan välisten tapaturmien lisääntymiseen. Työtapaturmista johtuvien sairauspoissaolojen määrä on noussut 143 päivällä. Työtapaturmista aiheutuneiden yliopistolle vakuutusyhtiön korvaamien poissaolopäivien määrä on noussut vain hieman edellisestä vuodesta (+15). Työntekijöiden työtapaturmat johtuvat pääosin kaatumisista, kompastumisista ja liukastumisista, joten sekä asunnon ja työpaikan välisillä matkoilla tapahtuviin tapaturmiin että kiinteistönhuoltoon on syytä kiinnittää huomiota. Työtapaturmien määrä on kasvussa, joten työtapaturmien syntymisen estämiseen ja jo sattuneista vahingoista oppimiseen on panostettava.



Kuvio 2. Työntekijöille sattuneet vahingot, korvatut vahingot ja työpaikkaturmat, tapaturmataajuus sekä yli 3 pv työkyvyttömyyden aiheuttaneet vahingot

Mielenterveyteen liittyvien poissaolojen määrä on vähentynyt 0,4 päivällä henkilöä kohden (1,8 pv/hlö) ja tuki- ja liikuntaelinsairauksista johtuvien sairauspoissaolojen määrä on pysynyt ennallaan alhaisella tasolla (0,8 pv/hlö).

Panostus henkisen työsuojelun toimintamallien juurruttamiseen ja psykososiaalisten voimavara- ja kuormitustekijöiden tasapainoon sekä työhyvinvoinnin kehittymiseen sekä johtajuuden että yksilön hallittavissa olevin keinoin jatkuu (työyhteisön hyvät tavat, vastuullinen työkäyttäytyminen, mielen- ja fyysisen hyvinvoinnin tukeminen, lähijohtajien tuki).

3.4.4 Työsuojelu ja työsuojelun kehittäminen 2024

Työsuojelun kehittäminen perustuu työn riskien arvioinnissa tunnistettuihin työn vaaroihin ja haittatekijöihin. Työn riskien arviointi ei vielä tuota selkeitä kehittämiskohteita, joten työsuojelun kehittäminen keskittyy edelleen työturvallisuuden rakenteita kehittävään työhön, aiempiin työsuojelun toimintaohjelman toimenpiteisiin ja työpaikkaselvityksistä ilmeneviin kehittämiskohteisiin.

Kehittämiskohteita vuonna 2024 ovat:

- Työn riskien arvioinnin toteuttamisen tuki yksiköille ja työpaikkaselvitysten kytkeminen osaksi työn riskien arviointia
    - Työturvallisuusvastuiden perehdytys osana varmennustoiminnan road show-tilaisuuksia (työsuojelupäällikkö)
    - Työn riskien arvioinnin toimintatavan sisällöllisen ohjeistuksen ja arvioinnissa hyödynnettävän Rego-järjestelmän teknisen ohjeistuksen laatiminen (työsuojelupäällikkö)
    - Lähijohtajan käsikirjan päivittäminen työsuojeluosaamisen osalta (työsuojelupäällikkö)
    - Koneiden ja laitteiden riskien arvioinnin kytkeminen työn riskien arviointiin (yksiköt)
- Kartoitus työpaikkaselvityksissä useimmin esille nousseiden kuormitustekijöiden pienentämisestä (työsuojelupäällikkö)
- Työsuojelutilastojen tarkentaminen työtapaturmailmoittamisen osalta (työsuojelupäällikkö)
- Työturvallisuuspätevyyksien hallinnan kehittämisen jatkaminen

Kaksi ensimmäistä kehittämiskohdetta on päätetty työsuojelutoimikunnan helmikuun 2024 kokouksessa ja päivitetään osaksi yliopiston työsuojelun toimintaohjelmaa.

3.5 Tietosuoja

3.5.1 Tietosuoja Jyväskylän yliopistossa

Jyväskylän yliopiston tietosuojapolitiikassa on määritelty ne pääperiaatteet, vastuut ja toimintatavat, joihin yliopisto on sitoutunut, jotta yksilöiden (rekisteröity) oikeudet ja vapaudet toteutetaan henkilötietojen käsittelyssä.

Yliopiston keskeisimmät henkilötietovarannot ovat:

- hr-tiedot (rekrytointi ja työntekijätiedot)
- laskutukseen ja maksatukseen liittyvät tiedot
- opiskelijoiden ja oppilaiden tiedot
- sidosryhmä ja asiakastiedot
- tilastointi
- päätöksenteko, asianhallinta ja kirjaamon arkisto
- turvallisuustekniset järjestelmät ja tietoturvan toteuttama valvonta sekä
- henkilötietoja sisältävät tutkimusaineistot

Yliopiston tulee noudattaa tietosuojaperiaatteita kaikessa toiminnassaan. Tietosuojaperiaatteet ovat:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus

Rekisterinpitäjä (yliopisto) on vastuussa henkilötietojen käsittelyn lainmukaisuudesta, eikä se voi ulkoistaa vastuutaan.

Rekisterinpitäjä on nimennyt yliopistolle tietosuojavastaavan, joka on sijoitettu organisatorisesti laki- ja hallintopalveluihin. Tietosuojavastaava hoitaa lakisääteisiä tehtäviään, joita ovat mm. seurata tietosuojasäännösten noudattamista, tuoda esiin havaitsemiaan puutteita sekä antaa tietoja ja neuvoja henkilötietojen käsittelystä johdolle ja työntekijöille. Tietosuojavastaava pyrkii toimissaan siihen, että rekisterinpitäjä pystyisi saavuttamaan riittävän tietosuojan tason (kypsyystaso). Myös laki- ja hallintopalveluiden lakimiehet osallistuvat tietosuojalainsäädännön toimeenpanoon ja avoimen tiedon keskuksen aineistonhallinta-asiantuntijat tutkijoiden ja opettajien kouluttamiseen sekä tietoturvatiimi tietoturvallisuuden kehittämiseen ja poikkeamienhallintaan. Tietosuojalla on rajapintaa myös mm. laadun- ja riskienhallintaan sekä turvallisuuteen.

Suomessa henkilörekisterilaki tuli voimaan 1.1.1988, sitä seurannut henkilötietolaki 1.6.1999 ja tietosuoja-asetus 25.5.2018. Henkilötietolaki perustui EU:n antamaan direktiiviin. Henkilötietojen käsittelyn lainmukaisuudella on siten pitkät perinteet.

3.5.2 Keskeiset tapahtumat edellisen raportin jälkeen

Keskeiset tapahtumat Euroopan unionin ja Suomen osalta

EU:n komissio antoi tiedonsiirtoja Yhdysvaltoihin koskevan vastaavuuspäätöksen 10.7.2023. Vastaavuuspäätöstä voidaan pitää merkittävänä, koska se helpottaa merkittävästi tiedonsiirtoja. Komission 4.6.2021 hyväksymät vakiosopimuslausekkeet edellyttävät erillisiä oikeudellisia arviointeja ja lisäsuojamekanismeista sopimista. Jos lisäsuojamekanismeja ei ole käsittelijän toimesta toteutettu EU lainsäädännön vaatimalla tavalla on tiedonsiirto voinut estyä. Näin kävi laajamittaisesti verkkosivuilla käytetyn Google Analyticsin osalta väliaikaisesti. Käytännössä yhdysvaltalaiset yritykset voivat siirtopäätöksen voimaantultua sertifioida itsensä osaksi siirtomekanismia (EU – U.S Data Privacy Framework DPF). Järjestelyn pysyvyydestä pitemmällä aikavälillä ei ole kuitenkaan varmuutta. Euroopan unionin tuomioistuin on katsonut komission kaksi edeltävää järjestelyä pätemättömiksi (ECLI:EU:C: 2015:650, ns. Schrems I tuomio 10.6.2015, Safe Harbour ja ECLI:EU:C:2020:559, ns. Schrems II tuomio 16.7.2023, Privacy Shield).

Kansallisen valvontaviranomaisen (ja Euroopan tietosuojavaltuutetun) tulkinta on, että pseudonymisoitu tieto on henkilötietoa, vaikka luovutuksensaaja ei pysty tunnistamaan rekisteröityjä saamastaan aineistosta. Tämä hankaloittaa mm. tehokkaasti pseudonymisoidun

tutkimusaineiston käsittelyä EU/ETA alueen ulkopuolella. EU:n yleisen tuomioistuimen ratkaisu (T-557/20, SRB v EDPS), joka annettiin 26.4.2023 olisi mahdollistanut tulkintalinjamuutoksen. Euroopan tietosuojavaltuutettu (EDPS) valitti kuitenkin päätöksestä EU:n tuomioistuimeen, jonka ratkaisua asiassa ei ole toistaiseksi saatu.

Suomen hallituksen hallitusohjelman mukaan hallitus toteuttaa kansallisen tietosuojalainsäädännön kokonaisuudistuksen. Kokonaisuudistuksen yhteydessä on tarkoitus hyödyntää tarvittaessa nykyistä laajemmin tietosuoja-asetuksen kansallista liikkumavaraa. Kokonaisuudistuksen yhteydessä on hallitusohjelman mukaan tarkoitus säätää hallinnolliset sakot tietosuojaloukkauksista koskemaan julkista ja yksityistä sektoria yhtäläisesti (kohta 6.4). Kokonaisuudistus on käynnistynyt joulukuussa 2023 ja koordinaatioryhmän toimikausi on vuoden 2026 loppuun.

Rekisterinpitäjiltä pyydettiin 2023 lausuntoja tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista. Euroopan komissio toimittaa Euroopan parlamentille ja neuvostolle joka neljäs vuosi kertomukset yleisen tietosuoja-asetuksen arvioinnista ja uudelleentarkastelusta. Tarvittaessa komissio voi esittää muutoksia asetukseen. Yliopisto nosti lausunnossaan esille kattavamman neuvonnan lisäksi mm. tarpeen ennakkopyyntö-/ennakkoratkaisumenettelyä vastaavasta järjestelystä.

Keskeiset tapahtumat Jyväskylän yliopistossa

Edellisessä varmennustoiminnantilan raportoinnissa asetettiin tietosuojatyölle useita kehittämiskohteita, joiden etenemistä tarkastellaan tässä kappaleessa viime vuoden osalta.

1. **Panostetaan pitemmän aikavälin kehittämiseen ja tunnistetaan keskeiset kehitystyötä edellyttävä osa-alueet osana digiturvaohjelmaa. Otetaan käyttöön julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), joka sisältää myös kriteerit tietosuojan toteuttamisen arviointiin.**

   Tämän kehittämiskohteen täyttämiseksi laadittiin yliopistolle digiturvaohjelma, jonka tietoturvan ja tietosuojan kehittämisryhmä hyväksyi. Ohjelma on vuosille 2023–2027. Alla olevassa taulukossa on kuvattu ainoastaan tietosuojan kehittämiskohteet ja niiden eteneminen (muut kehittämiskohteet ilmenevät tietoturvaraportoinnista).

Taulukko 1.

Nykytila	**Tavoitetila**	**Toimenpiteet**	**Eteneminen**
Puutteet vaatimustenmukaisuudessa, ei arviota.	Täytetään sääntelyn mukaisista vaatimuksista 80 % JulKrin mukaan.	Tarvittavien henkilöiden osallistuminen vaatimustenmukaisuuden arviointiin ja toimenpiteiden toteuttamiseen. Vuosittaiset itsearviot, joiden perusteella kehittämistoimien suunnittelu vuosittain. Ulkoinen arviointi ohjelmankauden loppuun mennessä.	Vaatimusten (mm. GDPR, tiedonhallintalaki) täyttymistä arvioitiin keväällä 2023 käyttäen JulKri-työkalua. Arviointi tehtiin itsearviointina tietoturvatiimin ja tietosuojavastaavan toimesta. Lievemmät poikkeamat on jätetty toistaiseksi huomioimatta (tietosuojan) kehityskohteina. Vakavat tietosuojapoikkeamat on nostettu lähivuosien vuosisuunnitelmiin: Yliopisto tunnistaa kaikki käsittelemänsä henkilötiedot. Yliopisto säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan, kun on tarpeen tietojen käsittelyn toteuttamista varten. Yliopisto pystyy osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia.
Digiturvan hallintamalli	Toimiva digiturvallisuuden ohjaus ja ajantasainen hallinnan kuvaus 2024. Tietosuojavaatimusten toteutumista pitää vastuuttaa, seurata ja raportoida.	Hankitaan digiturvan hallintaan työkalu. Päivitetään hallintamalli vastaamaan vähimmäisvaatimuksia pitäen ISO 27001 standardia viitekehyksenä (ml. ISO 27701:2021 laajennus). Jalkautetaan hallintamallin ylläpitovastuu. Varmistetaan ja tarvittaessa uudistetaan ohjausrakenteet.	Tietosuojan osalta ehditty aloittaa työkalun Digiturvamalli.fi testausta 2023. Käyttö jatkuu 2024.
Tietosuojan puutteellinen kypsyystaso, kypsyystasoa ei arvioida säännöllisesti.	Yliopisto saavuttaa riittävän tietosuojan	Valitaan arviointimetodologia, jota käytetään soveltuvin osin itsearviointiin.	Kypsyystason itsearviointi toteutetaan omana työnä ja se on aikataulutettu vuodelle 2024.

	kypsyystason ohjelmakauden loppuun mennessä.	Otetaan käyttöön tietosuojan vuosittainen kypsyystason itsearviointi 2024. Ulkoinen arviointi ohjelman loppuun mennessä 2027.	Välttämätön osa ulkoiseen arviointiin varautumista. Tutkimuksen tietosuojan kypsyystaso arvioitu KPMG:n toimesta 2019.
Nykytila	**Tavoitetila**	**Toimenpiteet**	**Eteneminen**
Tutkimusten henkilötietojen käsittelyn hallintamalli puuttuu. Tutkimuksen kehittämisohjelmaan mukaan Jyväskylän yliopistolla on olemassa yhtenäinen tutkimusaineistojen elinkaarenhallinta.	Tutkimuksia koskevien tietojen kirjaaminen ja ylläpito on selkeää. Täytetään vähintään lakisääteiset vaatimukset (seloste käsittelytoimista). Reaaliaikaisempi hallintamalli. Yliopisto tietää mistä tieteellisistä tutkimuksista se vastaa rekisterinpitäjänä, mikä on henkilötietojen käsittelyn elinkaarenvaihe ja mitä aineistoille tapahtuu tutkimuksen päätyttyä.	Tavoitteena digitaalinen seloste käsittelytoimista (2025). Opiskelijoiden asema rekisterinpitäjinä uudelleenarvioidaan (2023–2024).	Lakisääteiset vähimmäisvaatimukset täytetään todennäköisesti (seloste käsittelytoimista) jo nyt, mutta nykyinen toteutus ei tosiasiassa tue henkilötietojen elinkaaren hallintaa. Tutkimuksen tietosuoja ei ole vuoden 2024 kehittämiskohde. Toteutus aloittamatta.
Tietosuojaosaaminen/ tietoisuus ei jalkaudu ja vuoropuhelua tarvitaan enemmän. *Palaute Moodlen perehdytyksestä: Kuinka tarpeellisena pidät tietosuojakoulutuksen (4.65/5 erittäin tarpeellinen) *Pitäisikö edellyttää säännöllistä kertausta? Kyllä 89 %. Palautetta antoi 25 % vastanneista.	Tietosuojaosaaminen ja tietoisuus jalkautuu yksikkötasolle. Lisätään vuoropuhelua ja sen kautta osaamista. Tutkimusten projektipäällikköpalvelu tukee tietosuojan toteutumista yhteistyöhankkeissa (JY PI).	"Research privacy championit" tiedekunta /erillislaitos (kokeilu 2023, laajentaminen palautteen perusteella 2024). Yhteistyöhankkeiden tietosuojaohje 2024. CIPT sertifioitu työntekijä digipalvelut ohjelmakauden loppuun mennessä. OSC panostaa ohjaajien aineistonhallintakoulutuksiin 2023–2025. Merkittävä osaamisen, tietoisuuden ja vuoropuhelun	Research Privacy Champion kokeilu ei saanut kannatusta tietoturvan- ja suojan kehittämisryhmässä, joten sitä ei toteutettu 2023. Muuta ei esitetty tilalle vuoropuhelun lisäämiseksi. Projektipäällikköpalvelu on raportoinut edistävänsä ohjetta vuoden 2024 kuluessa. OSC on panostanut aineistonhallintakoulutuksiin 2023 lukien.

	Privacy by design & default teknisten vaatimusten tuki riittävää. Opinnäytetöiden ohjaajat osaavat ohjata henkilötietojen käsittelyssä. Laajempi ja monipuolinen tietosuojatiimi muotoutuu yhteistyön kautta.	lisääntyminen ohjelmakauden loppuun mennessä.	Aineistonhallinnan tuella, tutkimusetiikalla, tietosuojalla ja lakipalveluilla yhteinen Teams kanava tiedonvaihtoon. ”Sudenkuoppakoulutukset ” aloitettu 2023 (FAQ tutkijoille).
Nykytila	**Tavoitetila**	**Toimenpiteet**	**Eteneminen**
Tietosuojakurssin suorittaneita 32,2 %, hyväksyttyjä suorituksia 25,8 % koko henkilökunnasta. Palautetta antaneista 38.5% koki osaamisensa kasvaneen merkittävästi ja 51 % jonkin verran viime vuosina.	Esitys on ollut (2018 lukien) koulutusten pakollisuudesta. Pakollisuuden käyttöoikeuksiin sitomisesta.	Koulutuksen ja testien pakollisuus käyttöoikeuksien voimassaololle.	Johto päättää mitä koulutuksia toteutetaan tai tulee suorittaa (koulutusmateriaalit on laadittu ja ne ovat käytettävissä). Niitä voidaan hankkia tarpeen mukaan myös ulkopuolisilta. **Perusteet ovat säilyneet samoina 25.5.2018 alkaen:** Kyse on ensisijaisesti lakisääteisestä velvoitteesta eli organisatorisista suojatoimista. Jyväskylän yliopiston on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti (TsA 32 art). Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät: seurata, että noudatetaan tätä asetusta, mukaan lukien… käsittelyyn osallistuvan henkilöstön koulutus ja

			tähän liittyvät tarkastukset (TsA 39 art). Kun päätetään hallinnollisen sakon määräämisestä ja määrästä…on otettava huomioon seuraavat seikat: rekisterinpitäjän vastuun aste, ottaen huomioon…organisatoriset toimenpiteet (83 art).

2. **Aloitetaan säännölliset itsearvioinnit ja käyttöönotetaan kypsyystasomalli**

   Ensimmäinen säännölliseksi tarkoitettu itsearviointi (JulKri) toteutettiin 2023 ja sen tulokset raportoitiin tietoturvan- ja suojan kehittämisryhmälle. Kypsyystason arviointimalleista tutustuttiin AICPA/CICA privacy maturity malliin ja Uuden-Seelannin PMAF arviointimalliin. Myös Ranskan valvontaviranomainen (CNIL) on julkaissut arviointimallinsa, joka on saatavissa ainoastaan ranskaksi. Ensi vaiheessa 2024 tullaan käyttämään Uuden-Seelannin arviointipohjaa, koska AICPA/CICA mallin mukaista kartoitustyökalua ei ole mahdollista saada käyttöön ja ilman sitä AICPA/CICA mallista on hankala tuottaa järkevää raporttia. Kypsyystason arvioiminen on olennaista, jotta voidaan varautua ohjelmakauden lopun ulkoiseen arvioon.

3. **Pyritään suuntaamaan työpanosta enemmän tietosuojan kokonaishallinnan parantamiseen ja yhteistyöhön (pistemäisen ohjauksen vähentäminen ja yhteistyö OSC aineistonhallintakoulutusta antavien kanssa)**

   Tietosuojavastaava on pyrkinyt vähentämään tietosuojailmoitusten oikolukemista, koska niiden sisällöllinen korjaaminen edellyttäisi pääsääntöisesti koko tutkimussuunnitelman läpikäyntiä mahdollisten ristiriitojen havaitsemiseksi. Mallilomakepohjissa on annettu ohjeet niiden täyttämiseen ja tästä on tehty myös neuvontatallenteita. Kaikkiin informointia koskeviin kysymyksiin kuitenkin edelleen vastataan.

   Yhteistyötä OSC tutkimuksen tuen tiimin ja opetustiimin kanssa on lisätty. Opetustiimin kanssa tavattiin ensikertaa huhtikuussa 2023. Tutkimuksen tiimin kanssa yhteistyötä on ollut pidempään. OSC on kiitettävällä tavalla panostanut aineistonhallinnan ja ohjaajien koulutuksiin sekä digitaaliseen kehittämiseen. Voidaan todeta, että koulutusta on hyvin tarjolla sitä haluaville. Myös laki- ja hallintopalvelut järjestävät tutkijoille suunnattua koulutusta, tietopyyntökoulutusta ja anonymisointikoulutusta tilataan joka toinen vuosi.

   Tietosuojavastaava osallistui 2023 Keski-Suomen hyvinvointialueen eettisen toimikunnan yhteistyötapaamiseen, jossa oli aiheena tutkijoiden haasteet siinä, että rekisteröidyn informointi osattaisiin tehdä oikein. Keskustelua myös jatkettiin/jatketaan sairaanhoitopiirin tietosuojavastaavan kanssa. Henkilötietoja käsittelevien tutkijoiden tulisi ymmärtää

tietosuojavaatimukset ja osata soveltaa niitä omaan tutkimukseensa. Toisaalta voisi olla tarvetta myös yksinkertaistaa informointikäytänteitä.

Jyväskylän yliopiston tietosuojavastaava on mukana myös korkeakoulujen tietosuojavastaavien työvaliokunnassa, jonka kautta on mahdollista saada tietoa siitä, miten muissa korkeakouluissa tietosuojatyötä toteutetaan.

Kokonaisuudessaan henkilökohtaisen ohjauksen ja neuvonnan tarve ei ole toistaiseksi vähentynyt. Myös yhteistyön lisääminen luo uusia haasteita mm. neuvonnan yhdenmukaisuuden ja lähes reaaliaikaisen tuen tarpeen osalta.

4. **Toteutetaan tietosuojan vuosikello**

Viime vuodelle oli asetettu tavoitteeksi vuosikellon toteuttaminen, joka on ohessa. Tietosuojan vuosikello toteutettiin kuvaamaan kunkin kvartaalin keskeisiä työkokonaisuuksia, joita on toteutettu ohjauksen ja neuvonnan ohella. Tietosuojatöissä on vaihtuvuutta vuositasolla ja vain osa tehtävistä toistuu (koulutukset, arvioinnit, raportointi).

Kuvio 3. Tietosuojan vuosikello 2023

Whisteleblow, TalentAdore ja Secapp olivat vuoden 2023 merkittävimmät vaikutustenarviointien kohteet. Myös kouluttaminen ja tiedottaminen oli hyvällä tasolla.

5. **Otetaan käyttöön tietosuojatyötä ja sen hallintaa tukeva työväline tai vähintään kartoitetaan näiden tuottamat mahdollisuudet**

Kokeilukäyttöön saatiin Digiturvamalli työkalu, joka sisältää erilaisia tietoturvan ja tietosuojan vaatimuskehikoita, jotka on pilkottu tehtäviksi. Hyvin toteutettuna Digiturvamalli mahdollistaa paremman tietosuojaraportoinnin. Työkalun testaamien jäi vähäiseksi vuonna 2023. Työkalu

päätettiin kuitenkin hankkia käyttöön vuodelle 2024, jolloin sen hyödyntämistä pyritään jatkamaan.

6. **Jaetaan vastuuta ja aloitetaan uutta yhteistyötä osaamisen ja tietoisuuden kasvattamiseksi**

Tietoisuuden lisäämiseksi toteutettiin kuvituskuva tietoturvaloukkausten raportoinnista, joka toimitettiin tietoisuuden lisäämiseksi GRPR:n syntymäpäivänä työntekijöiden sähköpostiin. Samalla korjattiin tilanne ilmoittamisen osalta niin, että poikkeamailmoitusta varten käytössä oleva lomake on kunnossa ja löytyy HelpJYU palvelun etusivulta. Poikkeamaraportoinnista tullaan muistuttamaan vuosittain.

Normaalikoulun kanssa on suunniteltu kuvituskuvaa lasten informoimiseksi henkilötietojen käsittelystä ja se on tarkoitus toteuttaa vuoden 2024 keväällä.

Vastuiden jaossa on edelleen haasteita, eivätkä vastuut esim. järjestelmädokumentoinnissa, vaikutustenarviointien laadinnassa tai rekisteröityjen informoinnissa jalkautuneet riittävällä tavalla yliopistopalveluissa tai hankintoja tekevissä yksiköissä. On myös havaittu, että tiedekunnissa voidaan suunnitella esim. sovelluksia tai alustaratkaisuja henkilötietojen käsittelyyn kolmansien osapuolten lukuun, joiden tietosuojaa- tai tietoturvaa ei osata toteuttaa ja dokumentoida riittävällä tavalla. Näihin voidaan puuttua vasta, jos asia tulee ilmi jotakin kautta.

Rekisteröityjen tietosuojainformointien selkeyttämiseksi toteutettiin Legal Desing projekti yrityksen Dot. kanssa ajalla 11.5.2023 – 29.6.2023. Osana projektia uudistettiin opiskelijoiden tietosuojailmoituksen rakenne ja yleisilme. Vastaava toteutustapa kopioitiin kaikkiin pysyvien käsittelytoimien tietosuojailmoituksiin, jotka julkaistiin verkkosivu uudistuksen yhteydessä marraskuussa. Projektia lopputulosta pidettiin onnistuneena.

3.5.3 Tietosuojan tilannekuva

Tietosuojan tilannekuvassa yliopiston tasolla ei ole tapahtunut kokonaisuudessaan merkittävää muutosta edellisten raportointikierrosten jälkeen. Uutena haasteena on noussut esille tekoälyn hyödyntäminen, sen vaikutukset ja mahdollisuudet vääristää tietoa. Tässä kerrataan kuitenkin jo aiempina vuosina esiin tuodut puutteet, joita tietosuojavastaavan tehtävänä on nostaa esille.

Tietosuojan osalta toteutettiin ulkoinen kypsyystason arviointi tutkimuksen osalta KPMG:n toimesta vuonna 2019. Tuolloin tietosuojan tasoa pidettiin ”kehittyvänä” riittävän sijaan. Uusi arvio on tarkoitus toteuttaa digiturvaohjelman mukaisesti 2027. Uudelleenarviointiin on vielä aikaa, mutta tavoitteen saavuttaminen edellyttää vuositasolla tapahtuvaa merkittävää kehittämistä. Keskeistä tässä on se, että kokonaisarkkitehtuurityön resurssointi on kunnossa, eikä käy niin että ko. työ pysähtyy jälleen useiksi vuosiksi. Tarvitaan tuloksia.

Rekisterinpitäjän osoitusvelvollisuuden, rekisteröidyn oikeuksien toteuttamisen ja säilytysaikojen noudattamisen näkökulmasta on olennaista, että rekisterinpitäjä tunnistaa kaikki käsittelemänsä henkilötiedot. Tietosuojavastaava on raportoinut tätä koskevista puutteista ensimmäisestä tietotilinpäätöksestä lukien. Kokonaisarkkitehtuurin linjausprosessiin liittyvä yhdenmukainen dokumentointi (omistajuudet, tietojärjestelmät, käsiteltävät tiedot,

vaikutustenarvioinnit, tietoturva jne.) piti ottaa alun perin käyttöön 2021, mutta ensimmäinen käyttöönottovaihe on siirtynyt helmikuulle 2024 saakka.

Vaikka säilytysajat on pääsääntöisesti määritelty tiedonohjaussuunnitelmassa ne eivät välttämättä toteudu järjestelmätasolla. Järjestelmien kartoituksen jälkeen seuraava vaihe olisi kartoittaa sitä, miten niissä toteutetaan tietojen poisto säilytysajan päätyttyä. Uusi järjestelmiä, joiden käyttötarkoitusta ja säilytysaikoja ei ole määritelty (ml. automaattiset poistot) ei pitäisi ottaa tuotantoon. On myös havaittu tarvetta tehdä lisämäärittelyä osaksi tiedonohjaussuunnitelmaa (esim. HelpJYU). Jokaiselta järjestelmäomistajalta tarvitaan väistämättä myös omaa aktiivisuutta säilytysaikojen läpikäynnin osalta.

Tietosuojavastaava on saanut palautetta siitä, että tutkijoille ei ole sensitiivisten eli ns. erityisten henkilötietoryhmien käsittely-ympäristöä. Asia ei ole korjaantunut vuoden 2023 kuluessa, joten se on otettava myös osaksi tätä raporttia. Opiskelijoiden käytössä olevien käsittely-ympäristöjen riittävyys tulisi selvittää ja tarjottavat ympäristöt sekä mahdolliset puutteet tulisi tuoda selkeästi esille ja ohjaajien tietoon. Yliopiston tehtävänä on huolehtia siitä, että sen lukuun henkilötietoja käsittelevillä tutkijoilla on riittävän turvalliset työvälineet. Yliopiston tehdessä linjauksia sen tulisi myös varmistaa, että ne pystytään käytännön tasolla toteuttamaan. Tutkimusten elinkaarenhallinnassa on myös haasteita, koska arkistointia koskevat ratkaisut puuttuvat. Sen sijaan, että aineistot siirrettäisiin tutkimuksen päätyttyä arkistoon, yksittäinen tutkija toimii ”arkistona”. Arkistoa koskeva asia on edennyt jonkin verran loppuvuodesta 2023.

Edellä kerrottujen puutteiden sijaan täytyy myös mainita, että yliopistolla on hieno digitaalisen kehittämisen malli ja muuta digitaalista kehittämistä on tehty merkittävästi viime vuosina.

Tietoturvan osalta kaikki preventiivisen toiminta on tärkeää, jos tapahtuu tietovuoto, jälkikäteen, on tehtävissä hyvin vähän tilanteen korjaamiseksi.

Järjestelmien osalta, jotka on otettu käyttöön siten, ettei ole määritelty mitä henkilötietoja käsitellään ja mikä on esimerkiksi rekisteröidyn tarkastusoikeuden toteuttamistapa, oikeuksien toteuttaminen ei välttämättä vastaa tietosuoja-asetuksen vaatimuksia.

Tietosuoja- ja tietoturvakoulutuksen ja kertauksen tulisi olla jokaiselle henkilötietoja yliopiston lukuun käsittelevälle pakollista. Vuoden 2019 KPMG tarkastusraporttia lainatakseni (ja tulevaa arviointi ennakoiden) tulos voi olla yhtä huono kuin edellisellä kerralla: ” Dokumentoidun materiaalin ollessa pääasiallisesti kunnossa, arvioinnin yhteydessä todettiin, että merkittävimmät havainnot liittyivät tietosuojan jalkauttamisen ja implementoinnin puutteisiin. Lisäksi henkilöstön tietosuojatietoisuuden tasossa nähdään parantamisen varaa, johtuen osittain siitä, ettei laadittua ohjeistusta ole osattu hyödyntää tai paikantaa, ja tarjottuihin tietosuojakoulutuksiin ei ole osallistuttu.”

Tietosuojatyöllä on liittymäpinta myös tiedonhallintatyöhön ja kokonaisarkkitehtuuriin ja tietosuojan tulisikin jäsentyä osaksi yliopiston vielä toistaiseksi puuttuvaa tiedonhallintamallia.

Rekisteröidyn oikeuksia koskevat pyynnöt ovat pysyneet maltillisina. Lisäksi O365:ssä käyttöönotettu kaksivaiheinen tunnistautuminen on vähentänyt valvontaviranomaiselle raportoitavien tietoturvaloukkausten määrää. Valvontaviranomaisessa ei ole ollut 2023 vireillä

Jyväskylän yliopistoon rekisterinpitäjänä kohdistuvia valituksia. Yliopistolla on kuitenkin haasteita oikeuksien toteuttamisen osalta, koska tietovarantojen kartoitus on jäänyt muun digitaalisen kehittämisen jalkoihin. Tarkastuspyyntöjen määrän nopea kasvu vaikuttaisi merkittävästi yliopiston toimintaedellytyksiin sitoen ylläpitäjien työaikaa eli toiminta voisi potentiaalisesti lamaantua. Uusien käyttöönottojen yhteydessä pitäisi entistä tarkemmalla tasolla selvittää, kuinka tarkastusoikeus toteutetaan.

Taulukko 3.

Tietosuoja	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Rekisteröidyn oikeuksia koskevat pyynnöt	5	3	1	4	4	7
Tietojenkäsittelysopimukset			10	44	80	51
Yhteisrekisterinpitäjyyssopimukset				11	4	1
Tiedonluovutuspyynnöt (henkilötiedot)			19	50	36	38
Tietoturvaloukkausilmoitukset valvontaviranomaiselle					12	1
Muut selvityspyynnöt valvontaviranomaiselta (ei poikkeama)			1			1
*Jos lukumäärä puuttuu asia ei ole vielä ollut kirjaamon kirjausten piirissä. **Sopimuksia jäänyt todennäköisesti tekemättä, mikä voi kertoa siitä, etteivät tutkijat tiedä, milloin kyseessä on yhteisrekisterinpitäjyys.						

3.5.4 Tietosuoja ja tietosuojan kehittäminen 2024

Tietosuojan kehittämistä vuoden 2024 kuluessa on käsitelty jo kohdassa ”Keskeiset tapahtumat edellisen kehittämisen jälkeen”. Digiturvaohjelman perusteella laaditaan vuosisuunnitelmat, joissa kuvataan kunkin vuoden keskeiset kehittämiskohteet.

Osana KA-työtä rekisterinpitäjä tunnistaa kaikki käsittelemänsä henkilötiedot. Alkuvuodesta aloitetaan tietojärjestelmätietojen keräämisellä, jonka kautta saadaan kuva henkilötietojen käsittelyyn käytettävistä tietojärjestelmistä. Myöhemmässä kehityksessä tulisi tunnistaa, mitä käsiteltävä tieto on (ainakin päähenkilötietoryhmät).

Sen jälkeen selvitetään järjestelmäkohtaisesti, miten säilytysaikoja noudatetaan. Tavoitteena on, että rekisterinpitäjä säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan kuin on tarpeen.

Tietosuojan kypsyystason osalta tehdään itsearvio, jonka perusteella suunnataan kehittämistä osoitusvelvollisuuden parantamisen näkökulmasta kaikista puutteellisimpiin kokonaisuuksiin. Arvion tekeminen on yksi osoitus siitä, että organisaatio pyrkii täyttämään velvoitteensa.

Tietosuojatietoisuutta lisätään, muistuttamalla poikkeamienhallinnasta ja ilmoitusvelvollisuudesta tietosuoja-asetuksen syntymäpäivänä 25.5. Samalla muistutetaan verkkokoulutuksista ja toukokuun anonymisointikoulutuksista. Tietosuojakoulutukset on lisätty

alkuvuodesta osaksi uuden työntekijän perehdytysprosessi. Muun koulutuksen ja testauksen osalta edetään johdon päättämällä tavalla.

Myös tietosuojan proaktiiviseen huomioimiseen tietojärjestelmissä ja hankinnoissa pyritään vaikuttamaan hankintaohjeistuksen ja osana hankintaprosessia mahdollisen uudistuksen yhteydessä.

3.6 Tietoturva

3.6.1 Tietoturva Jyväskylän yliopistossa

Jyväskylän yliopiston tietoturvaperiaatteissa on määritelty keskeiset tavoitteet ja periaatteet, joiden mukaisesti tietoturvaa toteutetaan yliopistossa. Tietoturvaperiaatteissa on määritelty tietoturvaan liittyvät vastuut. Tietoturvaan liittyviä vastuita on niin jokaisella käyttäjällä ja opiskelijalla kuin ylimmällä johdolla. Rehtorin ja koko ylimmän johdon sitoutuminen tietoturvallisuuden varmistamiseen on välttämätöntä koko henkilöstön sitouttamiseksi.

Käsitteet tietoturva, kyberturva ja digiturvallisuus tarkoittavat puhekielessä tavallisesti samaa asiaa, vaikka ne määritelmällisesti eivät synonyymeja olekaan. Digiturvallisuus jakautuukin osa-alueisiin tietoturvallisuus, kyberturvallisuus, tietosuoja, jatkuvuuden hallinta ja riskienhallinta. Yliopistossa digiturvallisuuden käsite ei ole vakiintunut. Keskipitkän aikavälin (3–5 vuotta) suunnitelma on laadittu digiturvaohjelman nimellä. Näitä kolmea termiä tieto-, kyber- ja digiturvallisuus käytettäessä on käytännöllisintä ajatella niiden kattavan samat osa-alueet, jotka digiturvallisuuteen on määritelty kuuluvaksi. Käytännössä tietoturvalla tarkoitetaan tietojen, palveluiden, tietojärjestelmien, tietoliikenteen sekä toimintaympäristön ja -tapojen suojaamista tiedon saatavuutta, eheyttä ja luottamuksellisuutta uhkaavilta tekijöiltä.

Tietoturva toimintona on sijoitettu digipalveluihin, jossa tietoturvan kehittämisestä, arvioinnista ja valvonnasta vastaa kolmen hengen tiimi. Tietoturvatiimi suunnittelee ja toteuttaa erilaisia hallinnollisia, teknisiä ja muita toimenpiteitä tietoturvan varmistamiseksi. Tietoturvallisuuden toteutuminen edellyttää kuitenkin koko henkilöstön osallistumista. Tietoturvaan liittyvät uhkat kohdistuvat tyypillisesti ensimmäisenä ihmisiin, jotka tietoa käsittelevät joko digitaalisesti tai perinteisemmin keinoin. Siksi on tärkeää, että jokainen yliopistolainen tunnistaa ja ymmärtää työssään kohtaamia tietoturvauhkia. Tietoteknisten järjestelmien suojaukset ja erilaiset tekniset tunnistamis- ja valvontamekanismit muodostavat oman, mutta kuitenkin riittämättömän osan tietoturvallisuuden kokonaisuudessa.

Viitekehyksenä tietoturvan toteuttamisessa ja hallinnassa yliopistossa sovelletaan julkishallinnon tietoturvakäytänteitä ja ISO 27001 -standardia. Tietoturvallisuuden kypsyyttä yliopistossa arvioidaan Kyberturvallisuuskeskuksen tarjoaman kybermittarin avulla. Kybermittari on yliopistojen tietoturvaverkoston yhdessä valitsema kypsyysmittari ja se mahdollistaa yliopistojen välisen vertailun.

Yliopistojen tietoturvallisuustoimia sääntelee laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki TiHL 2019/906), EU:n tietosuoja-asetus (2016/679), tietosuojalaki (2018/1050) ja muutamat erityislait. Vaatimustenmukaisuus tiedonhallintalain näkökulmasta arvioidaan julkisen hallinnon tietoturvallisuuden arviointikriteeristöllä (JulKri). Vaatimustenmukaisuuden

ja kypsyyden arviointiin käytettävät välineet eivät ole ristiriidassa toistensa kanssa ja sisältävät osittain samoja vaatimuksia. Yhteneväisyys myös ISO 27001 -standardin kanssa on merkittävää.

3.6.2 Keskeiset tapahtumat edellisen raportin jälkeen

Digiturvaohjelman toimeenpano

Digiturvaohjelma kattaa vuodet 2023–2027. Ohjelma sisältää osa-alueet tietoturvallisuus, kyberturvallisuus, riskienhallinta, jatkuvuudenhallinta ja tietosuoja. Ohjelman keskiössä on vaatimustenmukaisuus tiedonhallintalain pohjalta ja valittujen viitekehysten mukaan. Riskienhallinta on rajattu koskemaan tietoon, sen käsittelyyn ja käsittelyyn käytettäviin palveluihin liittyviä riskejä sekä tietosuojan vaikutustenarviontiin. Toiminnan jatkuvuus sisältyy ohjelmaan digitaalisten prosessien ja palveluiden osalta.

Ohjelman ensimmäinen toimeenpanovuosi osoittautui juuri niin haasteelliseksi kuin ohjelman laadinnan yhteydessä oletettiin. Tiedonhallintalain vaatimusten osalta tavoitteeksi asetettua vakavien poikkeamien korjaamista ei saatu valmiiksi. Tiedonhallintalain toimeenpanon ja yleisesti tietoturvan ja -suojan työ perustuu toimintaympäristön tuntemiseen. Tämä tarkoittaa erityisesti yliopistossa käsiteltävän tiedon, tietovirtojen, prosessien, toimintojen sekä tietojärjestelmien ja erilaisten riippuvuuksien tuntemista ja dokumentointia. Järjestelmätietojen kerääminen on raportin laatimisen aikaan aluillaan ja se toteutetaan työnkulkuautomaatiolla (KA Vasara) osana kokonaisarkkitehtuurityötä. Muiden tietojen koostaminen toteutetaan myöhemmin ohjelman aikana, joka tarkoittaa tavoitteiden uudelleen aikataulutusta tältä osin.

Jatkuvuudenhallinnassa digipalveluissa jatkettiin varautumissuunnitelmien kirjoittamista tai päivittämistä. Työ ei ole edistynyt aivan toivotulla tavalla monien kehittämistehtävien ja muuten kiireellisiksi tunnistettujen tehtävien viedessä ylläpitäjien ja kehittäjien työaikaa. Keskeiseen tietotekniseen infrastruktuuriin liittyvän varautumissuunnitelman työstäminen saatiin alulle.

Ohjelman toteutumista on kuvattu taulukkomuodossa tämän luvun lopussa. Oheisessa kuvassa alkuperäinen digiturvaohjelman karkea suunnitelma tavoitteineen.

Kuvio 4. Digiturvaohjelman päätavoitteet

Vaatimustenmukaisuus (tiedonhallintalaki)

Kehittämistoimissa 2023 pyrittiin saamaan JulKrin vakaviksi poikkeamiksi tunnistettuihin vaatimuksiin kohdistuvat työt käyntiin siten, että tehtäviin liittyvät vastuut on tunnistettu ja määritelty, ratkaisutavat ja tavoitetaso on sovittu ja käytännön työ voidaan aloittaa. Kaikki tehtävät eivät ole kertaluonteisia vaan prosesseja.

Vaatimustenmukaisuuden toteutumista tiedonhallintalain mukaisesti arvioidaan julkisen hallinnon arviointikriteeristöllä (JulKri) itsearviona seuraavan kerran kevään 2024 aikana. Vuosisuunnitellun yhteydessä kriteeristöä käytiin läpi, nostettiin vakavien poikkeamien korjaavia toimenpiteitä vuosisuunnitelmaan siltä osin kuin nähtiin realistisena.

Tietoturvavalvonnan kehittäminen

Teknisen tietoturvavalvonnan kehittäminen on keskitetty tietoturvan tilannekuvaprojektiin (Tilkku). Vuoden 2023 aikana muodostettiin parempi kokonaiskuva valvontakohteista ja -tavoista. Kokonaisuus kuvattiin tietoturvavalvonnan arkkitehtuurikuvauksessa. Yliopiston tietotekninen ympäristö on erittäin laaja ja monimutkainen. Teknisen valvonnan toteuttaminen ei ole suoraviivaista eikä kustannustehokkaasti helppoa. Valvonnan toteutuksessa on tehtävä monenlaisia kompromisseja ja toisaalta valintaa sen välillä, mikä osa kehittämisestä ja valvonnasta voidaan tehdä itse ja mikä olisi järkevää hankkia yliopiston ulkopuolelta. Joka tapauksessa yliopiston oma osaaminen on taattava ja siten varmistettava toimintakyky hankalissa tilanteissa. Arkkitehtuurissa päädyttiin toteuttamaan valvonta hyödyntäen kahta eri teknologiaa. Hajautettu malli on myös kustannuksiltaan paras ratkaisu. Jako valvonnassa voidaan karkeasti tehdä Microsoftin pilviympäristön ja yliopiston omassa konesaliympäristössä pyörivien palveluiden välillä. Näiden valvontaan sovelletaan siis eri teknologioita. SaaS[1]-palveluiden valvonta palvelua tarjoavien yritysten varassa.

Loppukesästä 2023 julkistettiin CSC[2]:n kilpailuttama ja sen kautta korkeakouluille tarjottava ulkoinen CSOC[3]-palvelu, joka rajattiin koskemaan korkeakoulujen Microsoft-pilvipalveluita. Palvelun hinta on sidottu käyttäjämääriin ja valvontaa tarjotaan ympärivuorokautisesti vuoden jokaisena päivänä. Yliopisto ei palvelua hankkinut johtuen sen korkeasta vuosihinnasta ja toisaalta ratkaisemattomasta haasteesta ympärivuorokautisen valvonnan ja yliopiston virka-aikaan rajoittuvan reagointikyvyn välillä.

Poikkeamienhallinta

Osana tietoturvavalvonnan kehittämisprojektia käynnistettiin poikkeamienhallinnan ohjekokonaisuuden uudistaminen. Valvonnan operatiivisen toiminnan järjestäminen ja dokumentointi ovat osa poikkeamienhallinnan ketjua havaitessaan ja tunnistaessaan tietojärjestelmissä epätavalliset tapahtumat. Yliopiston kannalta haasteellista on se, että valvonta, kuten myös reagointi, tapahtuu virka-aikana. Rikollinen tai muu haitallinen toiminta ei ole aikaa tai paikkaan sidottua eikä rikollisilla muutenkaan ole pidäkkeitä hyökkäystensä masinoinnissa.

---

1 Software as a Service
2 CSC – Tieteen tietotekniikan keskus Oy
3 CyberSecurity Operation Center

Teknisesti poikkeamia selvitellään ja ratkotaan tietoturvatiimin ja ylläitäjien toimesta. Tätä toimintaa varten digipalvelut teki jo kesällä 2022 päätöksen perustaa virtuaalitiimi (CSIRT[4]), joka kutsutaan koolle vakavien tai kriittisten poikkeamien selvittämiseksi. CSIRT on teknisistä asiantuntijoista ja ylläpitäjistä muodostettu virtuaalitiimi, ns. nopean toiminnan joukot, joka vakavan tai kriittisen poikkeaman tapahtuessa vastaa hyökkäyksen torjunnasta, pyrkii estämään tilanteen eskaloitumisen ja lisävahinkojen syntymisen sekä tekee jälkikäteen selvitykset poikkeaman syistä. Virtuaalitiimi muodostuu tiimin vetäjästä ja nimetyistä ylläpitohenkilöistä keskeisiltä teknologia-alueilta sekä tietoturvan teknisestä asiantuntijasta. Varsinainen operatiivinen toiminta oli tarkoitus käynnistää ja vakiinnuttaa vuoden 2023 aikana. CSIRT-toimintaa ei kuitenkaan ole saatu käytäntöön digipalveluiden jatkuvan resurssipulan takia: päivittäiset tehtävät ja suunnitellut kehittämistehtävät ovat vieneet kaiken ajan. Toiminnan käynnistämiseen liittyy myös ratkaisemattomia kysymyksiä mm. virka-ajan ulkopuolella tapahtuvan työn ja hälytysvalmiuden järjestelyistä ja korvauksista.

Tällä hetkellä toiminta poikkeamatilanteissa virka-ajan ulkopuolella perustuu vapaaehtoisuuteen. Digipalveluiden ylläpitohenkilöstö on hyvin sitoutunutta hoitamaan ongelmatilanteita myös vapaa-ajallaan. Se ei kuitenkaan ole kestävä ratkaisu, jonka varaan voidaan jättäytyä, eikä toisaalta tarjoa reilua ratkaisua työntekijöiden näkökulmasta.

Poikkeamienhallinnan ohjekokonaisuuden uudistamisella pyritään tekemään näkyväksi koko poikkeamatilanteiden hallintaan liittyvät toiminnot ja viestintä. Teknisen poikkeamien käsittelyn lisäksi keskeiseksi muodostuu tilannejohdon toiminta. Poikkeamien hallinnan voi ajatella jakautuvan kolmeen tasoon: operatiivinen, tilannejohto ja kriisijohto. Kriisijohdon rooli muodostuu tärkeäksi kriittisten poikkeamien hallinnassa erityisesti, kun uhka kohdistuu laajasti koko yliopistoyhteisöön tai yliopiston toimintaedellytyksiin tai herättää julkista mielenkiintoa. Ohjeiden päivityksellä pyritään nämä eri tasot nivomaan kiinteämmin toisiinsa. Ohjeet pelkästään eivät riitä takaamaan toiminnan tuloksellisuutta, vaan tiedottamalla ja erityisesti harjoittelemalla ne saadaan osaksi organisaation toimintaa.

Osaamisen kehittäminen

Henkilöstölle on edelleen ollut tarjolla tietoturvan perehdytyskurssi Moodle-alustalla. Kurssi soveltuu kaikille yliopistossa jo työskenteleville ja yliopistoon uusina työntekijöinä tuleville. Osallistumisaktiivisuus tarkastelujaksolla 2017–2023 on edelleen riittämätön.

- henkilöstöstä tietoturvatestin on suorittanut sen avaamisen jälkeen hyväksytysti 1814 henkilöä (ed. raportti 1418, muutos +28 %) henkilöä, mikä on noin 53 % aktiivisista käyttäjistä (Huom! luvut eivät ota huomioon henkilöstön vaihtuvuutta)
- henkilöstön tietoturvakurssin tai -perehdytyksen on niiden avaamisen jälkeen lokakuusta 2017 alkaen kokonaisuudessaan suorittanut 765 henkilöä (ed. raportti 881, joka laskettu perehdytyskurssin testin mukaan eikä huomioi sitä, että testin on voinut tehdä käymättä koko kurssiaineistoa läpi)
- henkilöstön tietoturvakurssin tai -perehdytyksen osasuorituksia on niiden avaamisen jälkeen lokakuusta 2017 alkaen tehnyt 1399 henkilöä (ed. raportti 1373, muutos +2 %)

4 Computer Security Incident Response Team

Testin suorittamisen kynnys on matalampi kuin itse kurssimateriaalin läpikäyminen. Testin tarkoituksena on ollut antaa henkilöstölle mahdollisuus osoittaa perustietämys tietoturvasta. Pelkän testin suorittaminen ei kuitenkaan ole riittävä tapa varmistua osaamisesta varsinkin, kun kyberuhkat muuttuvat nopeasti.

Digiturvaohjelman ja joiden tärkeimpien osa-alueiden kehittämistuloksia ja suunnitelmia on kuvattu tietoturvaosion lopussa olevassa taulukossa, jonka pohjana on digiturvaohjelman tavoitteet.

3.6.3 Tietoturvan tilannekuva

Poikkeamat tarkastelujaksolla

Vuosi 2023 oli yliopistossa tietoturvapoikkeamien osalta yllättävänkin rauhallinen. Näkyvimpänä ja todennäköisimpänä uhkana oli ja voi edelleen pitää erilaisia tietojenkalastelukampanjoita. Niitä kohdistui yliopistolaisiinkin eri muodoissa ja laajuudessa viikoittain. Kalasteluihin lankeamisia tapahtui kuitenkin hyvin vähän. Kaksivaiheinen todentaminen (MFA[5]) oli tehokas suoja ja vaikka hyökkääjä saikin tunnuksia ja salasanoja haltuunsa, ei pääsyä palveluihin syntynyt yritysten kohdistuessa lähinnä Microsoftin ympäristöön.

Koko tarkastelujaksolla vuoden 2024 alku olikin sitten synkempi, kun yliopistoon kohdistui turvasähköpostiksi naamioitu kalastelukampanja. Hyökkääjä käytti sinänsä periteisiä kalastelutemppuja, mutta pystyi murtamaan kaksivaiheisen todentamisen käyttämällä kalastelusivulla kehittynyttä automatiikkaa (AitM[6]). Saatuaan yhden tunnuksen haltuunsa, hyökkääjä levitti kampanjaansa yliopiston sähköpostin sisällä käyttämällä haltuun saamaansa aitoa sähköpostiosoitetta. Kyseinen kampanja oli laaja ja kohdistui lukuisiin organisaatioihin niin Suomessa kuin muuallakin maailmassa.

Alla olevassa taulukossa tietoturvatiimin käsittelemien häiriöilmoitusten määrät vuosittain. Nykyinen tikettijärjestelmä (ServiceNow/HelpJYU) otettiin poikkeamailmoitusten teossa käyttöön 2020.

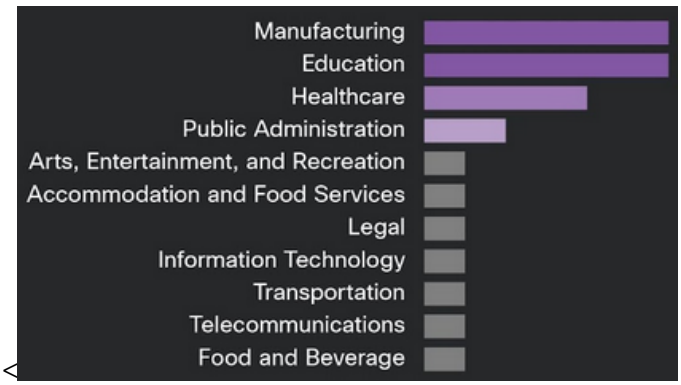
5 MultiFactor Authentication
6 Adversary in the Middle

Kuvio 5. Tietoturvapoikkeamailmoitukset

Yleinen kyberuhkatilanne

Tietojenkalastelu jatkuu edelleen aktiivisesti. Tekoäly tuottaa myös entistä uskottavampia kalasteluviestejä ja toisaalta tehostaa hyökkääjän automatisoituja prosesseja. Tyypillisesti kyberhyökkäykset alkavat sähköpostin välityksellä tapahtuvan kalastelun avulla. Haltuun saaduilla tunnuksilla hyökkääjä etsii reittiä organisaation arvokkaimpiin kohteisiin. Toisaalta suuri osa hyökkäyksistä on tarkoitettu nimenomaan tunnusten ja salasanojen keräämiseksi myytäväksi rikollisilla markkinoilla eteenpäin. Tunnukset ovat siis kauppatavaraa. Kaksi- tai monivaiheinen todentaminen ei enää takaa suojaa hyökkäyksiltä, mutta toki se edelleen on hyökkääjä hidastava suojausmekanismi. Kyberhyökkäysten toteuttaminen on rikollisille liiketoimintaa, jossa eri ryhmittymät myyvät hyökkäysteknologiaa, toteuttavat hyökkäyksiä palveluna tai myyvät käyttäjätietoja pimeillä markkinoilla.

Maailmanlaajuisesti suurinta huolenaihetta ovat aiheuttaneet kiristyshaittaohjelmat. Selvitysten mukaan yliopistot (laajemmin koulutussektori) ovat kiristyshaittaohjelmahyökkäysten suosituimpia kohteita yhdessä valmistavan teollisuuden kanssa.



Kuvio 6. Kiristyshaittaohjelmahyökkäysten jakautuminen toimialoittain (Lähde: Cisco Talos – Quarterly Trends, Jan 20224)

Lisäksi on muistettava, että yliopisto käyttää paljon ulkoisia palveluita, jotka myös voivat joutua hyökkäyksen kohteeksi ja siten vaikuttaa yliopiston päivittäiseen toimintaa. Tästä esimerkkinä on TietoEvryn Ruotsissa sijaitseviin palveluihin kohdistunut kiristyshaittaohjelmahyökkäys,

jonka seurauksena joidenkin ruotsalaisten yliopistojen palveluita on ollut pois käytöstä jo useamman viikon ajan (esim. palkanlaskenta). Yleinen periaate kiristyshaittaohjelman osuessa organisaatioon on, ettei hyökkääjien vaatimia lunnaita pidä maksaa. Kuitenkin vuonna 2023 lunnaita maksettiin maailmanlaajuisesti enemmän kuin koskaan, arviolta miljardi euroa. Niille, jotka lunnaita eivät maksaneet, kustannuksia aiheutui palveluiden palauttamisesta ja tuotantokatkoksista. Pahimmassa tapauksessa palautuksia ei voitu tehdä tai siihen ei oltu varauduttu ja yritys ajautui konkurssiin.

Varotoimena maailmalla havaittuihin hyökkäyksiin VPN-palveluita kohtaan yliopisto päätti toteuttaa omien VPN-yhteyksien kirjautumisiin kaksivaiheisen todentamisen. Käyttöönotot tehdään kevään 2024 aikana. MFA-laajentaminen yliopiston omiin palveluihin on edelleen jatkettava.

Kyberturvallisuuden kypsyys

Yliopistojen tietoturvaverkosto päätti vuoden 2021 syksyllä soveltaa Kyberturvallisuuskeskuksen kybermittaria yliopistojen kyberturvallisuuden kypsyyden arvioimiseen. Kybermittari on alun perin tehty huoltovarmuuskriittisten toimijoiden kyberkypsyyden arvioimiseksi, mutta se soveltuu minkä tahansa organisaation kypsyysmittariksi. Mittari perustuu kahteen amerikkalaiseen viitekehykseen (NIST CSF[7], DOE C2M28) ja on monelta osin yhteneväinen esim. ISO 27000 -standardin kanssa.

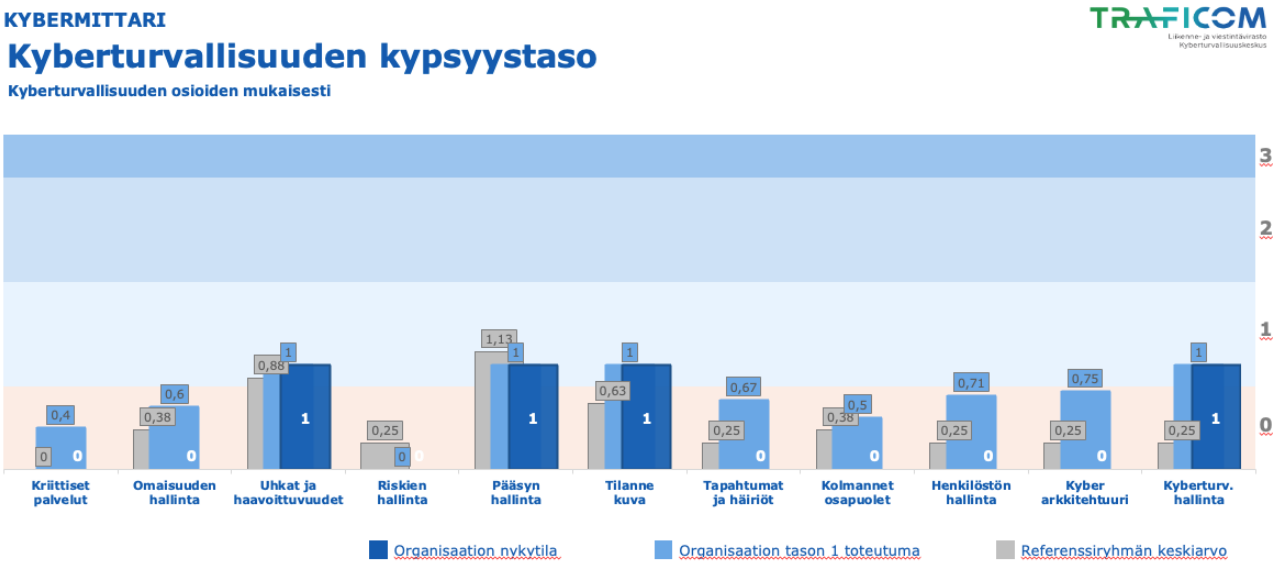
Kybermittariarviota ei ole päivitetty vuoden 2022 jälkeen, jolloin Jyväskylän yliopiston kypsyyttä arvioitiin Oulun ja Itä-Suomen yliopistojen vertaisarviona. Yliopistojen tietoturvaverkostossa on sovittu, että vertaisarviot uusitaan vuoden 2024 loppuun mennessä.

Edellisen arvion pohjalta tietoturvaverkosto on yhdessä valmistellut pohja-aineiston uhkamallinuksen ja poikkeamien hallinnan soveltamiseksi kussakin yliopistossa. Myös riskienhallinnan pohja-aineiston luominen saatiin alkuun, mutta se valmistuu vasta vuoden 2024 ensimmäisellä puoliskolla. Tehty yhteistyö helpottaa merkittävästi käytännön toteutusta.

Jyväskylän yliopiston digiturvaohjelmaan kirjattu kypsyystasotavoitteet on sovittu myös yliopistojen yhteiseksi tavoitteeksi. Tavoitteena on saavuttaa kypsyystaso 1 vuonna 2025 ja 2 vuonna 2027. Kyberturvallisuuskeskus pitää korkeakouluissa tasoa kaksi riittävänä.

Yliopistovertailussa (2022) Jyväskylän yliopiston tulokset asettuvat jonkin verran keskiarvoa korkeammalle. Erot eivät ole kovin merkittäviä ja kaavioidenkin perusteella on todettavissa, että yliopistot kamppailevat samankaltaisten haasteiden kanssa. Kunkin kypsyystason (1-3) saavuttamisen edellytyksenä on, että kaikki kyseiseen tasoon liittyvät vaatimukset täyttyvät. Alla olevassa taulukossa on vertailuun otettu Jyväskylän kypsyystason yksi täyttyneiden osiokohtaisten vaatimusten osuus:

7 National Institute of Standards and Technology, CyberSecurity Framework
8 Department of Energy Cybersecurity, Capability Maturity Model



Kuvio 6. Kypsyystason vertailu

Luottamusverkostot

Tilannekuvan ja uhkatiedon jakamisessa erilaiset yhteistyö- ja luottamusverkostot ovat keskeisessä roolissa. Yliopisto on aktiivisesti mukana ylipistojen tietoturvaverkostossa, joka muodostaa tärkeimmän luottamusverkoston. Kyseiseen verkostoon kuuluu myös CSC:n Funet CERT[9], joka valvoo Funet-verkkoa. Tiedonvaihto tapahtuu pääosin CSC:n pikaviestikanavilla ja kehittäminen on keskitetty työpajatoimintaan.

Vuonna 2023 perustettiin uusi kyberturvallisuuden koordinoima yliopistojen luottamusverkosto YO-ISAC[10]. Tiedonvälityskanavana toimii Traficomin pikaviestipalvelu. Yliopisto seuraa myös muita NCSC[11]-FI -kanavia haavoittuvuus- ja uhkatiedon keräämiseksi.

Vaatimustenmukaisuus

Vaatimustenmukaisuuden osalta keskeisimmät puutteet ovat edelleen tietoturvariskien ja jatkuvuuden hallinnassa. Riskienhallinnassa on tärkeää nojautua koko yliopiston riskienhallintapolitiikkaan ja -toimintatapoihin eikä luoda tietoturvariskien käsittelylle omaa menettelyä. Riskienhallinnan periaatteet on kuvattu varmennustoiminnan politiikassa. Se luo pohjan tietoturvariskien hallinnalle samoin kuin käyttöön otettu riskienhallintatyökalu.

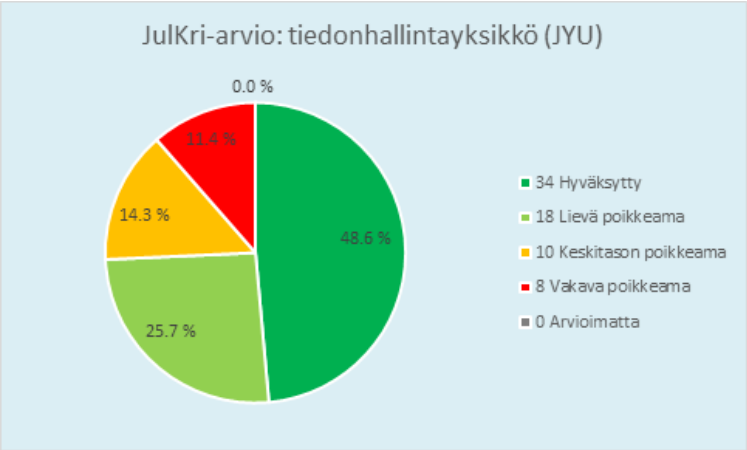
Tietoturvaan liittyviä riskejä arvioidaan jonkin verran tietosuojan vaikutustenarvioinnin yhteydessä. Toiminnan ja talouden suunnittelun yhteydessä tapahtuvassa riskienhallinnassa tietoturvariskit harvoin nousevat esiin, joka on sikäli hämmentävää, että suuri osa yliopiston toiminnoista nojautuu erilaisiin tietojärjestelmiin ja toisaalta tietoa voi pitää yliopiston merkittävimpänä omaisuutena. Tietoturvariskejä kirjataan jonkin verran tietoturvatiimissä

9 Computer Emergency Response Team
10 Information Sharing and Analysis Centre
11 National Cyber Security Centre

Exceliin, mutta riskit ovat tyypillisesti ongelmanratkaisutilanteisiin liittyvä, mutta sinänsä toki tarpeellisia kirjauksia ja käsittelyitä.

Digiturvaohjelmassa vaatimustenmukaisuuden osalta tavoitteeksi on asetettu, että vuoden 2023 loppuun mennessä 80 % kriteereistä on hyväksytty, keskitason poikkeamia on alle 5 % ja lieviä alle 15 %. Vakavia poikkeama ei tavoitteen mukaan olisi ollenkaan. Asetettu tavoitetaso oli vaativa ja optimistinen. Esimerkiksi suojattavien kohteiden ajantasainen dokumentointi sekä kohteiden välisten riippuvuuksien tunnistaminen ja dokumentointi edellyttää sekä kokonaisarkkitehtuurityöhön panostamista että koko organisaation sitoutumista tietojen koostamiseen.

Arviointituloksia ei ole päivitetty. Itsearvio uusitaan tämän vuoden jälkimmäisellä puoliskolla.



Kuvio 7. Tiedonhallintalain vaatimusten toteutuminen

Taulukko 3. JulKri-arviossa vakaviksi poikkeamiksi tunnistetut kohteet

Suojattavat kohteet	Organisaatio tunnistaa suojattavat kohteet sekä pitää niistä ajantasaista dokumentaatiota.
Suojattavat kohteet - riippuvuudet	Organisaatio on tunnistanut ja dokumentoinut suojattavien kohteiden väliset riippuvuudet.
Riskienhallinta	Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.
Asiakirjajulkisuuden toteuttaminen	Organisaatio varmistaa, että tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvän tietojenkäsittely suunnitellaan siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.
Jatkuvuusvaatimusten määrittely	Toiminnan ja siihen liittyvien olennaisten palvelujen ja tietojärjestelmien jatkuvuusvaatimukset on määritelty.
Käsiteltävien henkilötietojen tunnistaminen	Organisaatio tunnistaa kaikki käsittelemänsä henkilötiedot.

Säilytyksen rajoittaminen	Organisaatio säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan, kun on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten.
Osoitusvelvollisuus	Organisaatio pystyy osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia.

3.6.4 Tietoturva ja tietoturvan kehittäminen 2024

Julkishallinnon digiturvallisuuden kehittämistä tehdään Digi- ja väestötietoviraston työryhmissä. Yliopisto on mukana kolmessa työryhmässä. Yliopistojen yhteistä kehittämistä tehdään yliopistojen tietoturvaverkostossa.

Digiturvaohjelman toimeenpano

Digiturvaohjelma kattaa vuodet 2023–2027. Ohjelma sisältää osa-alueet tietoturvallisuus, kyberturvallisuus, riskienhallinta, jatkuvuudenhallinta ja tietosuoja. Ohjelman keskiössä on vaatimustenmukaisuus tiedonhallintalain pohjalta ja valittujen viitekehysten mukaan. Riskienhallinta on rajattu koskemaan tietoon, sen käsittelyyn ja käsittelyyn käytettäviin palveluihin liittyviä riskejä sekä tietosuojan vaikutustenarviontiin. Toiminnan jatkuvuus sisältyy ohjelmaan digitaalisten prosessien ja palveluiden osalta.

Digiturvaohjelman muut kuin tietosuojan päätavoitteet 2024:

- järjestelmätietojen kerääminen KA Vasaralla
- kyberturvallisuuden kypsyystasoarvion päivitys vertaisarviona
- digiturvallisuuden hallintamallin luominen
- kyberriskien tunnistamisen menettelyiden määrittely ja toteutus yksikkötasolla (TOP 3 riskiä)
- tietoturvavalvontakyvyn varmistaminen ja operatiivisen toiminnan vakiinnuttaminen
- henkilöstön ja opiskelijoiden tietoturvaosaamisen varmistaminen

Tarkemmat työsuunnitelmat on kirjattu digiturvaohjelman vuosisuunnitelmaan. Tietoturvan kehittämistoimenpiteet suunnitellaan digipalveluiden DUO-suunnittelun mukaisesti 3 kuukauden jaksoissa.

Digiturvan hallinta

Tietoturvan hallinta on kuvattu edellisen kerran 2017 laaditussa dokumentissa. Viitekehyksenä käytettiin ISO 27000 -standardia. Hallinnan kuvauksen ylläpitäminen Word-dokumentissa on työlästä ja jää helposti todellisesta tilanteesta jälkeen. Hallintaa helpottamaan yliopisto hankki vuoden 2024 alussa digiturvamalli.fi -palvelun. Palvelussa on valittavissa useita viitekehyksiä hallinnan toteuttamiseksi. Yliopistossa tietoturvan hallintamalli rakennetaan edelleen ISO 27000 -standardin pohjalta. Palvelussa toteutetaan myös tietosuojan hallinnan kuvaaminen tietosuoja-asetuksen perusteella. Hallintamalli tarjoaa valittujen viitekehysten pohjalta valmiit vaatimukset ja ehdotukset niiden toteutustavasta. Toimenpiteiden ja niiden näytön kirjaaminen on yksinkertaisempaa ja mahdollistaa toimenpiteistä vastaavien sitouttamisen, kun tehtävät osoitetaan suoraan heille (esim. haittaohjelmasuojaus työasematiimille).

Digiturvamalli helpottaa tulevia auditointeja, kun suuri osa tarkasteltavasta tiedosta on löydettävissä reaaliaikaisesti ylläpidetystä palvelusta. Koska palvelun käyttö on vielä aivan alussa, ei hallinnan tilaa vielä voi raportoida. Vuoden 2024 aikana valittujen viitekehysten toimenpiteistä tavoitteena on kirjata vähintään perustiedot.

Valvonnan kehittäminen

Teknistä tietoturvavalvontaa kehitetään luodun valvonta-arkkitehtuurin perusteella hajautettuna mallina. Vuoden 2024 aikana pyritään ottamaan valitut teknologiat tehokkaaseen käyttöön. Erityisesti Microsoft-ympäristössä valvontavälineitä kehitetään aktiivisesti ja mm. tekoälyavusteinen valvonta tai operointi voi tuoda merkittäviä etuja. Yliopiston omassa ympäristössä käytettävässä teknologiassa yliopisto on soveltanut koneoppimista jo jonkin aikaan. Tänä vuonna kyseisen kyvykkyyden todentaminen on keskeinen tavoite. Toinen keskeinen tavoite on hälytysjonon keskittäminen valvontalähteistä yhteen palveluun, jolloin seuranta olisi helpompaa. Teknisten parannusten ohella on hyvin keskeistä kehittää operatiivista toimintaa. Valvontajärjestelmien opettaminen (mm. false postive -hälytysten poistaminen) on hyvin henkilöintensiivistä työtä, joka rajoittaa tietoturvatiimin valvontaan liittyvien tehtävien hoitamista. Valvontaa on laajennettava ylläpidon puolelle.

Kehittämisen seuraavia askeleita (1-3 vuoden ajalla) on tarkasteltava myös kustannusten näkökulmasta. Vuoden aikana tehdään arvioita ja erilaisia kustannusskenaariota. Niiden yliopistojen kokemuksia, jotka ovat ottaneet käyttöön ulkoistetun 24/7 CSOC-palvelun, on seurattava tarkasti. Yleisesti tietoturvaan liittyvät ominaisuudet ovat muodostamassa merkittävän osan ohjelmistojen ja laitteistojen lisenssikustannuksista.

Henkilöstön ja opiskelijoiden tietoturvaosaaminen

Tietoturva- ja tietosuojakoulutusten pakollisuudesta on yliopistossa keskusteltu pitkään. Sitovaa päätöstä suuntaan tai toiseen ei toistaiseksi ole tehty. Keskustelussa rehtorin kanssa päädyttiin ratkaisuun, että pakollisuus käsitellään yliopistoin johtoryhmässä talven / kevään aikana. Pakollisuus on jo toteutettu muutamassa yliopistossa.

Tietoturvatestin tai -kurssin pakollisuus ei sellaisenaan ole riittävä tapa parantaa henkilöstön tietoturvatietoisuutta. Pakollisuus on kuitenkin tärkeä siksi, että se mahdollistaa edes jonkinlaisen kontrollin ja näytön henkilöstön tietoturvaosaamisen varmistamisesta. Lisäksi säännöllinen tiedottaminen, lyhyiden mikro-oppimisjaksojen tuottaminen tai pelillistetty kouluttaminen jatkuvana toimintona tehostaisivat oppimista ja kulttuurin kehittymistä.

Digiturvataidot antavat perustan digitaalisessa ympäristössä toimimiselle. Niiden voidaan sanoa olevan kansalaisten perustaitoja. Näin ollen on perusteltua ajatella, että yliopistotasoisissa opinnoissa käsitellään ja syvennetään tietoja ja taitoja, joita kybermaailman uhkien tunnistaminen edellyttää. Kun Jyväskylän yliopisto vielä tarjoaa alan opetusta, olisi luonnollista, että kaikki opiskelijat saavat laadukkaasti järjestettyä perehdytystä aiheesta. Tällä hetkellä yliopistoon tulevat uudet opiskelijat ohjataan pre-orientaatiokurssilla Moodle-oppimisalustalla myös tietoturvakurssille, jonka suorittaminen on pakollista. Toteutumista ei kuitenkaan voida valvoa eikä ole varmuutta siitä, että kaikki opiskelijat kurssin suorittavat. Digiturvallisuustaitojen opiskelu olisi järkevää lisätä kaikille opiskelijoille pakolliseksi osaksi

tutkintoa. Opetuksen toteutuksesta olisi luontevinta vastata IT-tiedekunnan eikä yliopiston hallinnon.

Taulukko 4. Digiturvaohjelman päätavoitteet ja niiden tilanne

Nykytila	**Tavoitetila**	**Toimenpiteet**	**Eteneminen**
Puutteet vaatimustenmukaisuudessa, ei arviota	Täytetään sääntelyn mukaisista vaatimuksista 80 % JulKrin mukaan	Tarvittavien henkilöiden osallistuminen vaatimustenmukaisuuden arviointiin ja toimenpiteiden toteuttamiseen Vuosittaiset itsearviot, joiden perusteella kehittämistoimien suunnittelu vuosittain Ulkoinen arviointi ohjelman loppuun mennessä	Perustietojen kerääminen sovittu pääarkkitehdin kanssa: • järjestelmätiedot 1H/24: käynnissä • tietoryhmät, prosessit, tilat: tehtävät siirretty 2025
Digiturvallisuuden kypsyystaso kybermittarin mukaan	Saavutetaan kypsyystaso 1 vuonna 2025, taso 2 vuonna 2027	Vuosittaiset itse- tai vertaisarviot, joiden perusteella kehittämistoimien suunnittelu Ulkoinen arvio ohjelman loppuun mennessä	Vertaisarvio 12/2024 mennessä
Digiturvan hallintamalli	Toimiva digiturvallisuuden ohjaus ja ajantasainen hallinnan kuvaus 2024.	Päivitetään hallintamalli vastaamaan vähimmäisvaatimuksia pitäen ISO 27001 standardia viitekehyksenä (ml. ISO 27701:2021 laajennus) Jalkautetaan hallintamallin ylläpitovastuu Varmistetaan ja tarvittaessa uudistetaan ohjausrakenteet	Hallintajärjestelmä digiturvamalli.fi hankittu ja otettu käyttöön, hallinnan rakentaminen aloitettu: tavoite 50 % standardin vaatimuksista kirjaukset
Riskienhallinta satunnaista ilman dokumentointia ja seurantaa	Prosessi ja työkalu, jotka jalkautettu sekä säännöllinen seuranta mitigoinneista 2024	Otetaan digiturvariskien hallinnassa käyttöön	REGO käyttöön vuoden loppuun mennessä myös tietoturvariskeissä

		yliopiston valitsema työkalu Kuvataan menettelyt ja jalkautetaan Raportoidaan riskeistä ja niihin kohdistuneista toimenpiteistä säännöllisesti	Menettelyt ja jalkauttaminen 2H/24
Rajallinen valvontakyky	Kyky ja resurssit valvoa identiteettejä, päätelaitteita ja sovelluksia	Varmistetaan valvontaan riittävä ja osaava henkilöstö Hankitaan riittävän kyvykkäät välineet (lisenssitasot) ja palvelut Jatkuva kehittäminen SOC-toiminta (sisäinen, ulkoistettu tai hybridi) 2026 vakiintunut	Tietoturvatiimissä keittämistä ja valvontaa tekevät henkilöt paikallaan. Operatiivista mallia laajennettava ylläpidon puolelle Työvälineet ok, lisenssitasot ja käsiteltävän datan määrä aiheuttaa kustannuksia
Kyberpoikkeamien hallinta järjestäytymätöntä	Operatiivinen CSIRT toiminnassa, sen kypsyystaso SIM3 mukaan 2024	Toimintatavat, vastuut, velvollisuudet ja vapaudet sovittu ja kirjattu Säännöllinen harjoittelu Itsearviomittarin (SIM3) soveltaminen	Ohjepäivitykset käynnistetty, tavoite 2Q/24 CSIRT ei toiminnassa, minimivaatimukset tavoitteena määritellä 2Q/24, jonka jälkeen uusi suunnitelma toiminnan aloittamisesta
Järjestelmien kriittisyyden arviointi pistemäistä, jatkuvuus- tai varautumissuunnitelmat puuttuvat tai ovat keskeneräisiä	Jatkuvuudenhallinnan prosessi ja menetelmät sekä kriittisyysluokitteluun menetelmä kuvattu 2023, luokittelu tehty ja jatkuvuus/varautumissuunnitelmat laadittu kriittisille järjestelmille 2025, säännöllistä harjoittelua 2027	Määritellään digipalveluille jatkuvuudenhallinnan prosessi Valitaan kriittisyysluokittelutyökalu Toteutetaan luokittelu Laaditaan tai viimeistellään jatkuvuussuunnitelmat	Jatkuvuudenhallinnan omistajuus epäselvä, minkä vuoksi prosessi määrittelemättä Digipalveluiden hallinnoimien järjestelmien kriittisyysluokittelu 3Q/24 (kevyt versio) Keskeisten opetuksen järjestelmien jatkuvuussuunnitelmat tehty, kriittisen

			infran osalta menossa
Tietoturvaosaaminen on puutteellista.	Henkilökunta osoittaa tietoturvaosaamisen vuosittain toistettavalla testillä ja suorittaa tietoturvan peruskurssin vähintään kolmen vuoden välein. Uudet työntekijät suorittavat aina tietoturvakurssin ja –testin. Uudet opiskelijat suorittava pakollisena tietoturvakurssin osana opintojaan.	Henkilökunta suorittaa testin hyväksytysti vuosittain alkaen 2023 Uudet opiskelijat suorittavat digiturvallisuuden perusteet osana tutkintoa lukuvuodesta 2023-2024 alkaen. Kaikki uudet työntekijät suorittavat osana perehdytystä tietoturvakurssin ja –testin vuodesta 2023 alkaen. Henkilökunta suorittaa tietoturvakurssin kolmen vuoden välein. Yliopiston johto määrittelee seuraukset suorittamattomista kursseista	Johto päättää mitä koulutuksia toteutetaan tai tulee suorittaa. Tilanne on epäselvä. Koulutusmateriaalit on laadittu ja ne ovat käytettävissä. Laadullista kehittämistä on suunniteltu vuodelle 2024.