Helsingin yliopiston identiteetin- ja käyttövaltuuksienhallinnan periaatteet

Versio 2, hyväksytty Tietotekniikkakeskuksen johtokunnassa 16.10.2018
Dokumentin on laatinut Päivi Pääkkö, Tietotekniikkakeskus

Sisältö

1. Yleistä....1
2. Periaatteet....3
3. Vastuut....5
4. Työntekijät....8
5. Opiskelijat....10
6. Kumppanit ja asiakkaat....10
7. Liitteet....11

1. Yleistä

Identiteetin- ja käyttövaltuuksienhallinnan periaatteiden tarkoituksena on mahdollistaa yliopistolaisille helppokäyttöinen ja turvallinen tapa kirjautua tarvitsemiinsa tietojärjestelmiin. Näitä periaatteita noudattamalla säästetään yliopistolaisten hallinnolliseen työhön käyttämää työaikaa sekä yksinkertaistetaan ja automatisoidaan käyttövaltuuksienhallintaan liittyviä prosesseja.

Identiteetin- ja käyttövaltuuksienhallinta koostuu erilaisista prosesseista, joiden mukaisesti Helsingin yliopiston tietojärjestelmien käyttäjiä ja heidän käyttövaltuuksiaan voidaan hallinnoida, käyttää ja seurata, sekä prosesseja tukevista teknisistä ratkaisuista. Tietojärjestelmien käyttäjät ovat Helsingin yliopiston omia työntekijöitä, opiskelijoita, asiakkaita tai kumppaneita, kuten muiden yliopistojen opiskelijat mm. Haka-federaation kautta, tai ulkoisten organisaatioiden käyttäjät. Tietojärjestelmät, joihin käyttövaltuuksia annetaan, voivat olla Helsingin yliopiston omia tietojärjestelmiä tai Helsingin yliopiston ulkopuolella käytettäviä palveluita, joihin käyttäjät tarvitsevat tehtäviensä hoidossa käyttövaltuuksia. Identiteetin- ja käyttövaltuuksienhallinnan tehtävänä on tehostaa käyttövaltuuksienhallintaa ja pienentää tietojärjestelmien väärinkäytön riskiä.

Tämä periaatedokumentti on tarkoitettu ohjeeksi sekä Tietotekniikkakeskukselle että kaikille tietojärjestelmien omistajille ja tietojärjestelmien hankintaan ja ylläpitoon osallistuville henkilöille. Periaatedokumentin tehtävänä on varmistaa, että identiteetin- ja käyttövaltuuksienhallinnan prosesseissa ja -teknisissä ratkaisuissa toteutuu Helsingin yliopiston etujen mukainen toiminta ja siten osaltaan suojella Helsingin yliopiston mainetta sekä edistää tietojärjestelmien positiivista käyttökokemusta. Identiteetin- ja käyttövaltuuksienhallinnan periaatteet tulee huomioida toimintamalleja ja tietojärjestelmiä kehitettäessä ja hankittaessa sekä arvioitaessa niiden toimivuutta ja sovellettavuutta.

Identiteetin- ja käyttövaltuuksienhallinnalle asetetut reunaehdot

Identiteetin- ja käyttövaltuuksienhallinnan periaatteiden pohjana ovat Helsingin yliopiston kokonaisarkkitehtuuriperiaatteet ja tietojenkäsittelyssä noudatettavat tietoturvaperiaatteet. Asianmukainen identiteetin- ja käyttövaltuuksienhallinta edellyttää lain ja asetusten, viranomaisvaatimusten, hyvän hallinnointitavan ja tietoturvan asettamien vaatimusten noudattamista. Periaatteita tulee arvioida vuosittain lainsäädännön ja muiden vaatimusten muutosten vaikutuksen suhteen.

Identiteetin- ja käyttövaltuuksienhallinta nojautuu mahdollisimman pitkälti oikeaa ja ajantasaista henkilötietoa tuottavien lähdejärjestelmien käyttämiseen. Tätä kautta identiteetinhallinta kytkeytyy useisiin yliopiston muihin henkilötietoa käsitteleviin prosesseihin. Identiteetinhallinnassa huomioidaan henkilötiedon masterdatan hallinnan periaatteet (Master Data Management, MDM). Osa identiteetinhallinnan käyttäjäjoukosta rajataan kuitenkin keskitetyn masterdatanhallinnan ulkopuolelle, mikäli se on tietosuojan vuoksi tarpeen.

Helsingin yliopiston tietojärjestelmien käyttäjäjoukko on erittäin laaja ja sisältää hyvin erilaisia käyttäjiä. Sekä käyttäjien lukumäärän että erityyppisten käyttäjien määrän voidaan olettaa kasvavan jatkossa. Käyttäjien suhde yliopistoon vaihtelee paljon, esimerkkeinä työsuhteessa oleva työntekijä tai alumnina toimiva entinen opiskelija. Erilaisilla käyttäjillä on hyvin vaihtelevia tarpeita ja näihin tarpeisiin liittyy erilaisia tietoturvariskejä, jotka tulee huomioida.

Identiteetin- ja käyttövaltuuksienhallintaan kuuluvat pääprosessit

Identiteetin- ja käyttövaltuuksienhallintaan liittyy suuri joukko prosesseja, joista oleellisimmat ovat:

- Uuden (digitaalisen) identiteetin luominen sekä käyttövaltuuksien myöntäminen ja luominen tietojärjestelmiin henkilön tullessa yliopistolle, esim. työsuhteen alkaessa tai kun opiskelija valitaan Helsingin yliopistoon
- Käyttövaltuuksien muuttaminen ja tarpeettomien käyttövaltuuksien poistaminen, käyttöperusteen päättyessä tai kun henkilön suhde yliopistoon muuttuu, esimerkiksi kun opiskelijasta tulee työntekijä, työntekijän työtehtävät muuttuvat tai työsuhde päättyy
- Käyttövaltuuksien hyväksymis-, valvonta- ja raportointikäytännöt
- Kansallisten ja kansainvälisten federaatioiden sekä sosiaalisen median tarjoamien kirjautumisratkaisujen hyödyntäminen, esimerkiksi toisen korkeakoulun opiskelija voi kirjautua oman kotikorkeakoulun käyttäjätunnuksella joihinkin Helsingin yliopiston tarjoamiin palveluihin

Tietotekniikkakeskus määrittelee prosessit sellaisiksi, että identiteetinhallinnalle asetetut reunaehdot täyttyvät. Prosessit pyritään pitämään mahdollisimman kevyinä, yhtenäisinä ja yksinkertaisina hallinnollisen työkuorman minimoimiseksi unohtamatta kuitenkaan perusvaatimuksia, joita ovat:

- Henkilö tunnistetaan asianmukaisesti
- Henkilö sitoutuu noudattamaan yliopiston tietojärjestelmien käyttösääntöjä ja hyväksyy yliopiston edellyttämät lisenssiehdot
- Henkilöllä on oltava sopimus tai puolto käyttövaltuudelle yliopiston prosessien mukaisesti
- Käyttövaltuudet ja henkilötiedot poistetaan, kun tarve sille päättyy

Prosessien kulkuun vaikuttaa mm. käyttäjän rooli ja kyseessä olevan järjestelmän turvallisuustaso.

Identiteetin- ja käyttövaltuuksienhallinnan ulkopuolelle rajatut kohteet

Tässä vaiheessa periaatteita sovelletaan vain tuotantoympäristöön, mutta periaatteiden soveltaminen myös muissa käyttöympäristöistä on suositeltavaa (esim. kehitys-, testi- ja koulutusympäristöt).

Tässä kohtaa ei oteta kantaa kulunvalvontaan fyysisten tilojen osalta, vaikka se monissa organisaatioissa otetaan osaksi käyttövaltuuksien hallintaa.

2. Periaatteet

Helsingin yliopiston identiteetin ja käyttövaltuuksienhallinnan periaatteet ovat:

- Yliopistolla on keskitetty identiteetti- ja käyttövaltuustieto sekä yhtenäiset toimintamallit
- Käyttäjätunnukset ja käyttövaltuudet hallinnoidaan roolipohjaisesti ja ne liitetään aina sopimukseen tai opinto-oikeuteen
- Jokaisella yliopistolaisella on yksi muuttumaton henkilökohtainen käyttäjätunnus, jota ei saa luovuttaa kenenkään muun käyttöön

Yliopistolla on keskitetty identiteetti- ja käyttövaltuustieto sekä yhtenäiset toimintamallit

Helsingin yliopistossa on oltava selkeä ja ajantasainen kokonaisnäkemys siitä, keitä henkilöitä yliopistolla on ja kenellä on mitäkin käyttövaltuuksia Helsingin yliopiston tietojärjestelmiin ja mitkä ovat perusteet myönnetyille käyttövaltuuksille. Kriittisten tai laajasti käytettyjen tietojärjestelmien osalta on saatava keskitetysti tieto kunkin identiteetin eli henkilön käyttövaltuuksista eri tietojärjestelmissä. Tämä tarkoittaa, että **käyttövaltuudet ja niiden hyväksyntätieto tallennetaan ja ylläpidetään keskitetysti** siten, että käyttövaltuustieto on tietoturvallisesti, helposti ja ajantasaisesti saatavilla hallinnointiprosessin eri osapuolille. Tieto on saatava selville identiteetti- ja järjestelmäkohtaisesti. Lisäksi on saatava historiatieto siitä, milloin rooli ja käyttövaltuus on myönnetty, ja kuka sen on hyväksynyt.

Helsingin yliopistossa **noudatetaan identiteetin ja käyttövaltuuksienhallinnassa yhtenäisiä toimintamalleja**. Käyttövaltuuksia hallinnoidaan siten, että **kaikilla samantyyppistä työtä tekevillä käyttäjillä on lähtökohtaisesti samat käyttövaltuudet**. Esimerkiksi Helsingin yliopiston omat työntekijät saavat identiteetin ja esimääritetyt käyttövaltuudet tullessaan Helsingin yliopiston palvelukseen yhtenäisellä tavalla ja työsuhteen päättyessä käyttövaltuudet poistetaan yhtenäisellä tavalla. Yhtälailla yhtenäisellä tavalla toimitaan kun työtehtävät ja käyttövaltuustarpeet muuttuvat. Myös opiskelijoiden sekä kumppani- ja asiakaskäyttäjien identiteettien hallinnassa toimitaan yhtenäisiä menettelyjä noudattaen.

Poikkeuksen tähän muodostavat ainoastaan rajatussa erilliskäytössä olevat tietojärjestelmät, joista ei ole tarkoituksenmukaista saada keskitettyä identiteetti- ja käyttövaltuustietoa. Esimerkiksi yksittäisen tutkimusryhmän käytössä olevan tietojärjestelmän käyttövaltuudet voidaan hoitaa täysin tietojärjestelmän pääkäyttäjän toimesta ilman, että niistä on tietoa keskitetysti. Tällöinkin on kuitenkin pyrittävä noudattamaan tämän dokumentin muita periaatteita ja lisäksi käyttövaltuudet on dokumentoitava. Näissäkin tapauksissa on kuitenkin aina pyrittävä noudattamaan identiteetin- ja käyttövaltuuksienhallinnan periaatteita sekä arvioitava kannattaisiko tietojärjestelmän käyttövaltuuksista tuoda tieto keskitettyyn IAM-järjestelmään (identiteetin- ja käyttövaltuuksienhallinnan tietojärjestelmä), vaikka käyttövaltuuksien hallinnointiprosessi tapahtuukin keskitetyn IAM-järjestelmän ulkopuolella.

Tällöin IAM-järjestelmästä saadaan keskitetysti ajantasainen tieto käyttäjien kaikista käyttövaltuuksista.

Käyttäjätunnukset ja käyttövaltuudet hallinnoidaan roolipohjaisesti ja ne liitetään aina sopimukseen tai opinto-oikeuteen

Käyttövaltuudet niputetaan mahdollisimman pitkälle rooleihin, jolloin käyttäjät voivat saada suurimman osan tarvitsemistaan käyttövaltuuksista ilman erillistä hakuprosessia. Roolien lisäksi käyttäjille voidaan erikseen hakea lisää rooleja tai käyttövaltuuksia esimerkiksi sijaisuuksissa, projektiluontoisissa tehtävissä tai toimittaessa jaettuna resurssina useammassa organisaatioyksikössä.

Kaikki roolit ja käyttövaltuudet liitetään aina sopimukseen tai opinto-oikeuteen, jotta ne voidaan antaa ja poistaa sopimuksen tai opinto-oikeuden voimassaolon mukaan. Sopimuksia voivat olla HR-järjestelmästä tulevat sopimukset (esim. työsopimus), opintohallinnon tietojärjestelmästä tulevat opinto-oikeudet (esim. opinto-oikeus Avoimen yliopiston kurssille) tai epäviralliset muihin käyttäjiin liittyvät sitoumukset (esim. kutsu tutkimusryhmän jäseneksi). Sopimus on joko tuleva, voimassa oleva tai päättynyt ja tällä sopimuksen tilalla on vaikutusta henkilön rooleihin ja käyttövaltuuksiin. Esimerkiksi henkilö voi saada osan käyttövaltuuksista, jos hänellä on tulossa oleva työsopimus tai opinto-oikeus. Vastaavasti sopimuksen päätyttyä voidaan käyttövaltuudet poistaa vaiheittain. Tämä tarkoittaa myös, että työsuhteen päättyessä työntekijällä ei ole enää työntekijän rooliin liittyviä käyttövaltuuksia Helsingin yliopiston tietojärjestelmiin. Kun käyttäjätunnus, rooli tai käyttövaltuus päättyy, voidaan sulkemista kuitenkin viivästää (esim. 2 viikkoa), jotta käyttäjä ehtii ennen käyttövaltuuden lopullista päättymistä tehdä tarvittavat toimet esim. solmia uuden sopimuksen yliopiston kanssa. Tavoitteena on vähentää turhaa käsityötä esim. Helpdeskissä. Viivästykset sovitaan yhdessä tietojärjestelmien omistajien kanssa. Automaattisesti toteutettavia viivästyksiä ei koskaan sovelleta ns. pakkosuljentatapauksessa.

Yksittäisellä **henkilöllä tulee olla käyttövaltuudet lähtökohtaisesti vain hänen (työ)tehtävissään tarvitsemiin tietojärjestelmiin**. Vaarallisia rooli- ja käyttövaltuusyhdistelmiä vältetään. Vaarallisilla rooli- ja käyttövaltuusyhdistelmillä tarkoitetaan niitä rooli- ja käyttövaltuusyhdistelmiä, joissa yksittäinen käyttäjä saa käyttövaltuuksien yhdistelmän, joka on tarkoitettu eri ihmisille ja jossa prosessin tai järjestelmän kontrolli on uhattuna. Tällöin käyttäjä voi toiminnallaan saavuttaa jotakin etua muihin käyttäjiin nähden. Esimerkiksi jos henkilö toimii jonkin asian (esim. rahoitus, laskut, hankinnat, opinto-oikeudet) hakijana ja hyväksyjänä. Vaarallisia rooli- ja käyttövaltuusyhdistelmiä tarkastellaan sekä tietojärjestelmäkohtaisesti että prosessikohtaisesti yli tietojärjestelmärajojen. Vaaralliset rooli- ja käyttövaltuusyhdistelmät tulee ehkäistä työtehtävien asianmukaisella eriyttämisellä, eriyttämistä tukevilla käyttövaltuusmäärityksillä ja käyttövaltuuksien hyväksymiskäytännöillä sekä valvonnalla.

Jokaisella yliopistolaisella on yksi muuttumaton henkilökohtainen käyttäjätunnus, jota ei saa luovuttaa kenenkään muun käyttöön

Jokaisella käyttäjällä on yksi identiteetti ja yksi käyttäjätunnus yliopiston tietojärjestelmiin, vaikka hän toimisi monessa eri roolissa yliopistolla, esimerkiksi henkilö on sekä opiskelija että

työntekijä. Poikkeuksen muodostavat tietojärjestelmien ylläpito- ja pääkäyttäjätehtävät (katso seuraava kohta), yritysten edustajat (kuten vuokratyöntekijät) sekä rajatussa erilliskäytössä olevat tai vierailijakäyttöön kohdistetut tietojärjestelmät (esim. tutkimuksen tietojärjestelmät) tms. poikkeustilanteet.

Omaa käyttäjätunnusta, salasanaa ja muita tunnistusvälineitä ei saa luovuttaa toiselle henkilölle edes tilapäisesti. Perustellusta ja dokumentoidusta syystä voidaan tarvittaessa kuitenkin käyttää useamman henkilön käytössä olevia yhteiskäyttötunnuksia sekä järjestelmän sisällä olevia tai tietojärjestelmien väliseen kommunikointiin tarkoitettuja järjestelmätunnuksia. Yhteiskäyttö- ja järjestelmätunnuksille on aina nimettävä vastuuhenkilö joka huolehtii käyttäjätunnuksen asianmukaisesta käytöstä.

Yliopisto päättää käyttäjätunnuksen muodon eikä sitä vaihdeta, ellei siihen ole poikkeuksellisen painavaa syytä. Mikäli sama henkilö palaa takaisin yliopistolle oltuaan välillä hetkellisesti poissa, hänelle annetaan käyttöön sama käyttäjätunnus. Käyttäjätunnukseen liitetyt järjestelmäkohtaiset tiedot (esim. sähköpostit) on kuitenkin saatettu hävittää riippuen poissaolon pituudesta. Pitkän, useita vuosia kestävän poissaolon jälkeen käyttäjä saa uuden käyttäjätunnuksen. **Käyttäjätunnuksia ei kierrätetä** eli samaa käyttäjätunnusta ei koskaan anneta toiselle henkilölle, koska käyttäjätunnusta käytetään yleisesti tietojärjestelmissä yksilöimään käyttäjä.

Ylläpitäjillä ja pääkäyttäjillä on hyvä olla erillinen henkilökohtainen käyttäjätunnus tietojärjestelmässä heidän toimiessa ylläpitäjän tai pääkäyttäjän roolissa kuin heidän käyttäessä tietojärjestelmää tavallisena käyttäjänä. Ylläpito- ja pääkäyttäjätunnukset tulee olla erityisseurannassa. Vaihtoehtoisesti ylläpito- ja pääkäyttäjätehtäviä voidaan suorittaa henkilön normaalilla käyttäjätunnuksella, mutta silloin kirjautumisessa on käytettävä normaalia vahvempaa tunnistusmenetelmää (esim. Multi-factor authentication tai Suomi.fi-tunnistuspalvelu).

3. Vastuut

Yksikön toimintaan liittyvät vastuut

Yksiköiden johtajat

Yksikön johtaja vastaa yksikkönsä toiminnasta. Tähän sisältyy vastuu hyvän hallintotavan ja identiteetin- ja käyttövaltuuksienhallinnan periaatteiden toteutumisesta yksikössä.

Esimiehet

Esimies vastaa siitä, että työntekijän rooli- ja käyttövaltuustiedot ovat ajan tasalla. Lisäksi esimiehet käynnistävät oman ryhmänsä toimintaan liittyvien vierailijoiden käyttäjätunnusprosessin.

Yliopistopalveluiden palvelukoordinaattorit

Palvelukoordinaattoreiden vastuulla on tarkistaa perusteet vierailijoiden käyttäjätunnusprosessissa.

Käyttäjät

Kaikkien käyttäjien on noudatettava yliopiston tietojärjestelmien käyttösääntöjä. Lisäksi käyttäjän on raportoitava esimiehelleen tai Helpdeskille, mikäli havaitsee, että itsellä tai jollakulla muulla on vääriä käyttövaltuuksia johonkin järjestelmään.

Tietojärjestelmiin liittyvät vastuut

Tietojärjestelmän omistaja

Tietojärjestelmän omistaja vastaa siitä, että tässä dokumentissa määritellyt identiteetin- ja käyttövaltuuksienhallinnan periaatteet toteutuvat kyseisessä tietojärjestelmässä. Omistajan on otettava huomioon tietojärjestelmän turvallisuustaso, erityistarpeet sekä mahdolliset laillisuusnäkökohdat. Tietojärjestelmän omistaja määrittelee yhdessä identiteetinhallintapalvelun omistajan kanssa sen, miten käyttövaltuudet ja vaaralliset käyttövaltuusyhdistelmät kyseisessä tietojärjestelmässä hallitaan. Tietojärjestelmän omistaja myös vastaa tietojärjestelmän käyttövaltuuksien (myös pääkäyttäjävaltuudet) ajantasaisuudesta.

Tietojärjestelmän pääkäyttäjä

Tietojärjestelmän pääkäyttäjä vastaa käyttövaltuusmäärityksistä, niiden toteutuksesta ja tarvittaessa hyväksymisistä, säännöllisen inventoinnin toteuttamisesta sekä tietojärjestelmän mahdollisesti tarvitsemista järjestelmätunnuksista tietojärjestelmän omistajan ohjeiden mukaan.

Roolin vastuuhenkilö

Jokaiselle roolille nimetään vastuuhenkilö, joka vastaa roolin määrittelystä sekä niistä prosesseista ja ehdoista, joilla kyseinen rooli saadaan. Roolimääritykset tapahtuvat yhdessä roolin vastuuhenkilön, identiteetinhallintapalvelun omistajan ja tietojärjestelmien omistajien kanssa. Mikäli roolille ei alkuvaiheessa löydetä sopivaa vastuuhenkilöä, nimetään identiteetinhallintapalvelun omistaja vastuuhenkilöksi.

Ydintietojen hallintaan liittyvät vastuut

Identiteetin- ja käyttövaltuuksienhallinta nojautuu mahdollisimman pitkälti oikeaa ja ajantasaista henkilötietoa tuottavien lähdejärjestelmien käyttämiseen. Tämän vuoksi on tärkeää, että henkilötietoihin liittyvät ydintiedot ovat ydintiedon hallintamallin mukaisesti laadukkaita ja niitä käsittelevät henkilöt tekevät työnsä huolellisesti. Erityisen tärkeää identiteetinhallinnan näkökulmasta katsottuna on oikea ja ajantasainen tieto työntekijän henkilötiedoista, työsuhteen alkamis- ja päättymispäivästä, työtehtävästä, organisaatioyksiköstä, esimiehestä ja pitkistä

poissaoloista sekä opiskelijan henkilötiedoista, opinto-oikeuden alkamis- ja päättymispäivästä, läsnäolosta ja koulutusohjelmasta.

Henkilöstö-ydintiedon ydintietovastaava

Henkilöstö-ydintiedon ydintietovastaava vastaa työntekijöiden, apurahatutkijoiden, dosenttien ja emerituksien osalta henkilöiden henkilö- ja työsopimustietojen ajantasaisuudesta ja laadusta sekä määrittelee HR-prosessien käytäntöjä siten, että tässä määritellyt identiteetin- ja käyttövaltuuksienhallinnan periaatteet täyttyvät.

Opiskelija-ydintiedon ydintietovastaava

Opiskelija-ydintiedon ydintietovastaava vastaa opintohallinnon tietojärjestelmästä saatavien henkilöiden henkilö- ja opinto-oikeustietojen ajantasaisuudesta ja laadusta sekä määrittelee opiskelija-tietojen käsittelyyn liittyviä prosesseja siten, että tässä määritellyt identiteetin- ja käyttövaltuuksienhallinnan periaatteet täyttyvät.

Muu henkilö-ydintiedon ydintietovastaava

Muu henkilö-ydintiedon ydintietovastaava vastaa kumppani- ja asiakaskäyttäjien (muiden kuin opiskelijoiden, työntekijöiden, apurahatutkijoiden, dosenttien ja emerituksien) henkilö- ja sopimustietojen ajantasaisuudesta ja laadusta sekä määrittelee kumppani- ja asiakashenkilöiden käsittelyyn liittyviä prosesseja siten, että tässä määritellyt identiteetin- ja käyttövaltuuksienhallinnan periaatteet täyttyvät.

Muut vastuulliset tahot

Tietosuojavastaava

Tietosuojavastaava huolehtii ohjeistuksen ja neuvonnan avulla, että yliopistolla tapahtuvassa henkilötietojen käsittelyssä noudatetaan soveltuvaa kansallista ja kansainvälistä lainsäädäntöä sekä tietosuojaohjeistusta ja -käytäntöjä. Tietosuojavastaava valvoo henkilötietojen käsittelyä koskevien rekisterinpitäjän velvoitteiden noudattamista ja yksityisyydensuojan toteutumista tietojärjestelmissä ja toimintaprosesseissa sekä välittää tiedot tietosuojaan liittyvästä ohjeistuksesta identiteetinhallinnan prosessin eri osapuolille.

Tietoturvapäällikkö

Tietoturvapäällikkö osallistuu tietoturvallisuuden kehittämiseen, ylläpitämiseen ja ohjeistamiseen. Tietoturvapäällikkö vastaa tietojärjestelmien turvallisuustasoista sekä yksittäistä tietojärjestelmää laajempien vaarallisten rooli- ja käyttövaltuusyhdistelmien hallinnasta. Identiteetinhallinnan osalta hän välittää tiedon tietoturvallisuuden ohjeistuksesta ja muutoksista identiteetinhallinnan eri osapuolille.

IAM-palvelun omistaja

IAM-palvelun omistaja vastaa yliopiston keskitetystä identiteetin-, käyttövaltuuksien- ja pääsynhallinnan tietojärjestelmästä ja prosesseista sekä roolitietojen hallinnasta kokonaisuutena. IAM-palvelun omistaja vastaa myös henkilön perustietojen osalta MDM-periaatteiden noudattamisesta sekä huolehtii osaltaan kansallisten ja kansainvälisten säädöksien noudattamisesta, esimerkiksi Haka-federaation asettamista vaatimuksista.

IAM-palvelun omistaja määrittelee prosessit ja kriteerit, joilla ulkoinen tietojärjestelmä otetaan mukaan keskitettyyn identiteetin- ja käyttövaltuuksienhallintaan. Tämä sisältää sekä identiteettien että käyttövaltuuksien siirtämisen kohdejärjestelmiin (provisioinnin) että keskitettyihin kirjautumispalveluihin liittymisen.

IAM-palvelusta vastaava palvelupäällikkö

Identiteetin- ja käyttövaltuuksienhallinnasta vastaava palvelupäällikkö vastaa tästä identiteetin- ja käyttövaltuuksienhallinnan periaatedokumentista, sen ajantasaisuudesta ja siinä tapahtuvien muutosten tiedottamisesta ja toimeenpanosta.

Tietohallintojohtaja

Tietohallintojohtaja vastaa Tietotekniikkakeskuksen toiminnasta ja siten myös IAM-palvelusta.

4. Työntekijät

Tämän politiikan mukaiset menettelyt on löydyttävä henkilön työhönottoon ja työstä lähtöön liittyvistä käytännöistä ja prosessikuvauksista.

Uusi työsuhde

Käyttövaltuuksien saaminen edellyttää, että

1. työntekijän tiedot ovat HR-järjestelmässä ennen työsuhteen alkamista
2. työntekijälle on lisätty hänen tehtävien mukaiset roolit IAM-järjestelmässä
3. työntekijä on tunnistettu asianmukaisesti käyttäjätunnuksen saamisen yhteydessä

Jokainen työntekijä saa työntekijä-roolin automaattisesti työsopimustietojen perusteella ja siihen liittyvät käyttövaltuudet mm. intranetiin, sähköpostiin ja oman kotihakemiston.

Käyttövaltuuksia ja rooleja ei kopioida suoraan toiselta työntekijältä uudelle työntekijälle, vaan jokaisen työntekijän kohdalla tarpeet on arvioitava erikseen.

Työtehtävien muutokset

Kun työntekijä siirtyy samassa yksikössä toisiin tehtäviin tai toiseen yksikköön Helsingin yliopistossa, käyttövaltuudet arvioidaan kokonaisuudessaan ja ne muutetaan uuden tehtävän ja/tai organisaatioyksikön mukaisiksi. Yksittäiset käyttövaltuudet poistuvat ja ne pitää hakea ja hyväksyä uudestaan, mikäli niille on edelleen tarvetta. Vanhat käyttövaltuudet pidetään voimassa kohtuullisen siirtymäajan (esim. 4 viikkoa).

Esimiehen tehtävänä on tarkistaa vuosittain (esim. kehityskeskustelun yhteydessä), että työntekijän rooli- ja käyttövaltuustiedot ovat ajan tasalla.

Poissaolot työsuhteen aikana

Työntekijällä säilyy perus IT-palvelut työstä vapautuksen aikana, esimerkiksi käyttäjätunnus, yliopiston sähköposti ja pääsy HR-järjestelmässä omiin tietoihin. Sen sijaan sensitiivisempään tietoon työntekijällä ei ole pääsyä työstä vapautuksen aikana, esimerkiksi muiden henkilöiden tiedot opiskelijarekisterissä tai HR-järjestelmässä. Muutokset työntekijän käyttövaltuuksissa toteutetaan asteittain kohtuullisen siirtymäajan sisällä (esim. 4 viikkoa) työstä vapautuksen alkamisesta.

Kaikkia työstä vapautettuja kohdellaan lähtökohtaisesti samalla tavalla riippumatta siitä miksi työntekijä on työstä vapautettuna (esim. opintovapaa vs. perhevapaat). Poikkeukset hoidetaan erillisen päätöksen ja manuaaliprosessin mukaan. Esimerkiksi jos kysymyksessä on työtehtävistä pidättäminen tai muu vastaavanlainen tilanne (ns. äkkilähtötapaukset), käyttövaltuudet suljetaan välittömästi.

Työntekijällä säilyy kaikki käyttövaltuudet lomien ja sairaspoissaolojen aikana. Poikkeukset (esim. useamman kuukauden poissaolot) hoidetaan erillisen päätöksen ja manuaaliprosessin mukaan.

Työsuhteen päättyminen

Keskitetyn identiteetinhallinnan kautta määritellyt roolit ja käyttövaltuudet liitetään työntekijän työsopimukseen. Ne poistetaan asteittain työsuhteen päättymisen jälkeen kunnes lopulta koko käyttäjätunnus passivoidaan neljän viikon kuluttua työsuhteen päättymispäivästä. Samalla tavalla annetaan heräte mahdollisille manuaaliprosesseille. Tällä on merkitystä erityisesti, jos kyseinen työntekijä jatkaa esimerkiksi opiskelijana tai emerituksena ja säilyttää sitä kautta käyttäjätunnuksen, mutta käyttövaltuudet pitää saada vastaamaan uutta opiskelijan tai emerituksen roolia. Irtisanottujen tapauksissa noudatetaan nopeutettua menettelyä.

Esimiehen on huolehdittava siitä, että työntekijä antaa työnantajalle kuuluvan oleellisen materiaalin, kuten esim. sähköpostit ja tiedostot, esimiehelle ennen työsuhteen päättymistä. Työntekijän käyttäjätunnusta ei luovuteta esimiehelle materiaalin saamiseksi myöhemmin.

5. Opiskelijat

Opiskelijakäyttäjien kohdalla noudatetaan yleisesti samoja periaatteita kuin mitä on lueteltu yliopiston työntekijä käytön osalta, mutta koska opiskelijat poikkeavat vastuiden ja valvonnan suhteen työntekijöistä, on lisäksi huomioitava seuraavat seikat:

- Opiskelijan käyttövaltuudet sidotaan opiskelijan opinto-oikeuteen ja läsnäoloilmoittautumiseen.
- Opiskelija saa käyttövaltuudet roolipohjaisesti.

6. Kumppanit ja asiakkaat

Helsingin yliopistolla kumppaneiksi ja asiakkaiksi käsitetään ne henkilöt, joilla ei ole HR-järjestelmästä saatavaa työsopimusta tai opintohallinnon tietojärjestelmästä saatavaa opinto-oikeutta yliopistoon. Tällaisia voivat olla esimerkiksi apurahatutkijat, dosentit, emeritukset, siviilipalvelusmiehet, konsultit, alumnit, tutkimusverkostojen jäsenet, muiden korkeakoulujen opiskelijat ja henkilökunta kansallisten- ja kansainvälisten käyttäjätunnistusfederaatioiden kautta sekä erilaisten palveluntarjoajien, järjestelmätoimittajien ja yhteistyökumppanien käyttäjät. He toimivat täysin tai osin Helsingin yliopiston tietoteknisessä infrastruktuurissa ja käyttävät Helsingin yliopiston tietojärjestelmiä.

Kumppaneiden ja asiakkaiden osalta identiteetinhallinnan politiikassa noudatetaan samoja periaatteita kuin aiemmin on kuvattu. Tässä luvussa on kuvattu vain poikkeamat yleisestä identiteetin- ja käyttövaltuuksienhallinnan periaatteista.

Kumppaneille ja asiakkaille **ei ole olemassa vain yhtä tietojärjestelmää, josta heidän henkilö- ja sopimustiedot olisi saatavissa** IAM-järjestelmään. Heidän osalta käyttövaltuudet perustuvat kuitenkin aina johonkin kyseisen henkilön tai hänen edustamansa organisaation kanssa tehtyyn sopimukseen, opiskeluoikeuteen tai sitoumukseen. Käyttövaltuuteen oikeuttavana seikkana voi olla myös esimerkiksi palvelusopimus, yhteistyöverkoston toiminta tai väliaikainen työvoiman tarve. Kumppaneiden ja asiakkaiden henkilö- ja sopimustietojen hallinnasta päättää tarkemmin 'muu henkilö' ydintiedon ydintietovastaava.

Prosesseissa täytyy huomioida, että käyttäjien kytkentä yliopistoon ja heidän sopimuksensa tyyppi vaihtelee hyvin suuresti. Esimerkiksi satunnaiselle vierailijalle voidaan antaa pääsy yliopiston langattomaan verkkoon ilman vahvaa tunnistusta hyvinkin kevyellä prosessilla. Toisena ääripäänä on sensitiivistä tietoa sisältävän tietojärjestelmän ylläpitovaltuus esimerkiksi ulkopuoliselle konsultille, jonka saamiseksi edellytetään huomattavasti tiukempaa kontrollia, kuten vahvaa tunnistusta ja salassapitosopimuksen allekirjoitusta ylläpitotunnuksen saamiseksi.

7. Liitteet

IAM-järjestelmän dokumentaatio

https://wiki.helsinki.fi/display/IAMasioita

Kokonaisarkkitehtuuriperiaatteet

https://flamma.helsinki.fi/portal/home/sisalto?_nfpb=true&_pageLabel=content_view&contentId=HY320995&placeId=HY362329&lang=fi

Tietojärjestelmien käyttösäännöt

https://www.helsinki.fi/fi/it/tietojarjestelmien-kayttosaannot

Tietosuojaan liittyvä materiaali

https://flamma.helsinki.fi/fi/HY365467

Tietoturvan säännöt ja ohjeet

https://flamma.helsinki.fi/portal/home/sisalto?_nfpb=true&_pageLabel=pp_list&placeId=HY053674

Ydintiedon hallintamalli ja vastuut

https://wiki.helsinki.fi/display/a/Ydintiedon+hallintamalli+ja+vastuut