Voimaan: 1.10.2020	Vahvistaja: tietoturvapäällikkö Riitta Gröhn

A9 PÄÄSYNHALLINTA

SISÄLLYS

1 Pääsynhallinnan yleiset periaatteet

Tietoihin ja tietojärjestelmiin pääsyä rajoitetaan. Osana tietojen ja tietojärjestelmien suojaamista on myös rajoitettu pääsyä niihin tiloihin, joissa tietoa käsitellään.

Oikeus käyttää Aalto-yliopiston tietojärjestelmiä, lukuun ottamatta julkisia palveluita, on vain pääsyoikeuden saaneilla henkilöillä ja vain siinä määrin kuin henkilöllä on tarve tietää ja käyttää. Pääsyoikeudet liitetään aina johonkin käyttäjätunnukseen. Käyttäjätunnustyypit on kuvattu tämän dokumentin osiossa käyttäjätunnukset.

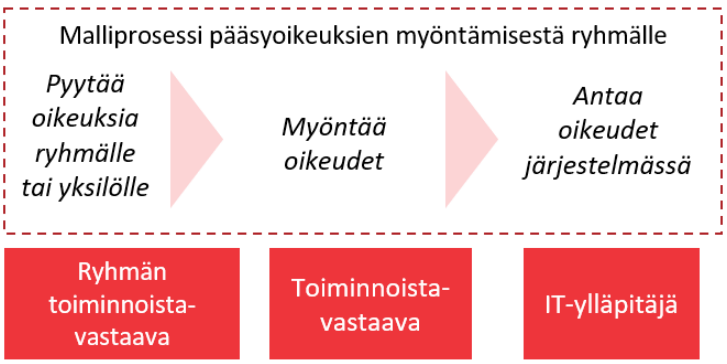
Pääsy tiloihin, joissa säilytetään luottamuksellista tietoa tai laitteita, esim. konesali ja tilat, joissa ylläpidetään konesalin palveluita, on rajoitettua. Vain niillä henkilöillä, joilla on tehtävänsä tai toimensa vuoksi tarve päästä kyseiseen tilaan on pääsy tällaisiin tiloihin ja kulkua tiloihin valvotaan tarkoituksenmukaisella tavalla. Tiettyihin alueisiin liittyy erityisiä rajoituksia. Ks. lisää A11 Fyysinen turvallisuus ja ympäristön turvallisuus.

1.1 Pääsyoikeuksien myöntämis-, muuttamis- ja poistamisvaltuudet

Pääsyoikeuksien myöntämis-, muuttamis- ja poistamisvaltuudet on vain nimetyillä henkilöillä. Vain tehtävään erikseen valtuutetuilla henkilöillä on Aalto-yliopistossa oikeus rekisteröidä käyttäjiä ja sallia pääsyoikeuksia, muuttaa tai poistaa niitä. Pääsyoikeuden myöntäjällä on oltava toiminnoista vastaavan valtuutus myöntää pääsyoikeuksia kohteeseen.

a) Pääsyoikeuden myöntämisprosessi käyttäjälle

b) Pääsyoikeuden myöntämisprosessi ryhmälle



c) Eskalaatioprosessi ryhmille

d) Eskalaatioprosessi yhdelle käyttäjälle

Kohtien c ja d eskalointimalliprosessit kuvaavat tilannetta, jos käyttäjälle tai käyttäjäryhmälle ei ole myönnetty oikeuksia tietoon tai tietojärjestelmään heidän pyynnöstään. Eskalointiprosessissa toiminnoista-vastaava, toiminnoistavastaavien ryhmä ja tarvittaessa tietty ohjausryhmä käsittelevät pääsyoikeuspyynnön uudestaan.

Pääsyoikeuksien (kulkuoikeuksien) myöntämisestä fyysisiin tiloihin, joissa suojattavaa omaisuutta säilytetään, on linjattu velvoittavassa ohjeessa A11.

1.2 Pääsyoikeuksien poistaminen ja muuttaminen

Pääsyoikeuden poisto estää pääsyn verkkoihin, verkkopalveluihin ja tietojärjestelmiin. Pääsyoikeuksien muuttamisessa ja poistamisessa noudatetaan niitä periaatteita, jotka on esitelty tämän dokumentin osassa pääsyoikeuksien ja käyttäjätunnuksien poistaminen.

Kulkuoikeuksien muuttaminen tai poistaminen estää pääsyn fyysisiin tiloihin. Kulkuoikeuksien poistamisessa noudatetaan A11:n mukaista menettelyä. Lähtökohtaisesti kuitenkin, jos pääsyoikeuksia muutetaan voi myös kulkuoikeuksien muuttaminen olla tarpeen.

1.3 Pääsynhallintaprosessi on dokumentoitu ja läpinäkyvä

Pääsyoikeudet tietoon ja tietojärjestelmiin, niitä muutetaan ja ne poistetaan kirjallisen prosessin mukaisesti.

Pääsynhallintaprosessi on läpinäkyvä, mikä tarkoittaa sitä, että tehdyistä pääsynhallintaan liittyvistä päätöksistä voidaan kommunikoida tarvittaville tahoille. Läpinäkyvyydellä pyritään takaamaan, että päätökset pääsynhallintaan liittyen ovat yhdenmukaisia.

1.4 Pääsynhallinnan ohittaminen ylläpito- ja hallintasovelluksilla

Normaalisti kaikki pääsy järjestelmiin, myös ylläpitotarkoituksessa, tapahtuu käyttäen pääsynhallintaa, jolloin käyttäjä voidaan yhdistää hänen toimintoihinsa. Jos pääsynhallinnan ohittaminen tai pääsynhallinnan ohittavien apuohjelmien käyttö on tarpeen, rajataan tällainen toiminta välttämättömään.

1.5 Salasanojen käyttö

Salasanojen hallintajärjestelmän on edellytettävä vahvojen salasanojen käyttöä. Käyttäjän on käytettävä yksilöllistä salasanaa, jonka on täytettävä laadulliset kriteerit. Salasanan laatukriteereistä ks. Salasanaohje. Samoja salasanoja ei saa käyttää uudelleen ja käyttäjä on pakotettava vaihtamaan salasanansa tietyin väliajoin ja tarvittaessa. Käyttäjän tulee huolehtia siitä, että ulkopuoliset eivät saa tietää hänen salasanaansa. Salasanoja ei saa tallettaa järjestelmissä selväkielisinä, eikä niitä saa lähettää sähköpostissa muutoin kuin salattuina.

Käyttäjän tulee vaihtaa salasana heti ensimmäisen kirjautumisen jälkeen, ellei salasanaa ole luovutettu sellaista teknistä ratkaisua käyttäen, jossa vain käyttäjä saa tietää salasanan (esim. password.aalto.fi). Joka tapauksessa salasana on kuitenkin vaihdettava säännöllisesti. Salasana vaihdetaan myös, jos muut syyt, kuten epäilys salasanan joutumisesta vääriin käsiin antavat sille aihetta.

1.6 Palvelinvarmenteet

Varmenteita käytetään, uusitaan ja suljetaan kirjallisten ohjeiden mukaan. Ajan tasalla olevista ja suljetuista varmenteista pidetään kirjaa.

1.7 Lähdekoodin ja konfiguraatioiden suojaaminen

Pääsyä ohjelmien, järjestelmien ja laitteistojen lähdekoodeihin ja konfiguraatioihin on rajoitettava niiden eheyden ja luottamuksellisuuden

turvaamiseksi. Lähdekoodeihin ja konfiguraatioihin tehtävät muutokset on lokitettava ja kirjausketju talletettava Aalto-yliopiston lokisääntöä noudattaen.

1.8 Pääsynhallinnan lokituksen tavoite ja lokien suojaaminen

Pääsynhallinnan tulee kerätä kirjautumislokia, jonka avulla voidaan yhdistää käyttäjä hänen kirjautumistoimiinsa. Lokien keräämisessä noudatetaan Aalto-yliopiston lokisäännössä määriteltyjä menettelyjä.

Pääperiaatteena on kuitenkin se, että lokitallenteiden kattavuus on oltava riittävä tietomurtojen tai niiden yritysten havaitsemiseen ja jälkikäteiseen todentamiseen. Lokitallenteet on suojattava ja estettävä niiden jälkikäteinen muokkaus. Myös lokitietojen säilytyksessä noudatetaan Aalto-yliopiston lokisääntöä.

2 Käyttäjätunnukset

2.1 Henkilökohtaiset käyttäjätunnukset

a) **Pääsyoikeudet ovat henkilökohtaiset ja ne on sidottu yksilölliseen ja henkilökohtaiseen käyttäjätunnukseen.**
Käyttäjätunnuksen avulla käyttäjä voidaan yhdistää toimintoihinsa ja vastuu voidaan kohdistaa häneen. Käyttäjätunnuksen avulla voidaan selvittää henkilön pääsyoikeudet yksittäisiin järjestelmiin. Käyttäjätunnuksilla sallitaan yksityinen käyttö kohtuullisissa määrin, mutta tälle käytölle on asetettu rajoituksia. Rajoitukset on yksityiskohtaisella tasolla kuvattu velvoittavassa ohjeessa A8, mutta lähtökohtaisesti sallittua käyttöä on esimerkiksi internetin selailu.

b) **Käyttäjä on tunnistettava luotettavasti.**
Ennen kuin käyttäjälle voidaan luovuttaa Aalto-tunnukset, on hänet tunnistettava luotettavasti. Esimerkiksi virallisesta henkilötodistuksesta tai tunnistautumisen on tapahduttava Aalto-yliopiston sähköistä palvelua käyttäen.

c) **Tunnistautumistiedot luovutetaan vain tunnistautuneelle henkilölle**
Uudet, korvaavat tai tilapäiset tunnistautumistiedot luovutetaan vain tunnistautuneelle (vahva sähköinen tunnistautuminen tai virallinen kuvalla varustettu henkilöllisyystodistus/passi) henkilölle.

d) **Pääsyoikeus voi antaa käyttäjälle luku- tai kirjoitusoikeuden järjestelmään.** Järjestelmästä ja henkilön roolista tai tehtävästä riippuen käyttäjällä voi olla järjestelmään vain lukuoikeus tai luku- ja kirjoitusoikeus. Esimerkiksi, oletuksena kaikilla aaltolaisilla on lukuoikeus Aalto.fi:n ”vain aaltolaisille” -materiaaliin, mutta tehtävien vaatiessa, voidaan käyttäjälle myöntää kirjoitusoikeus, jolloin käyttäjä voi luoda ja muokata Aalto.fi:n sisältöä.

Tunnusten luovuttamisen sähköisesti on aina tapahduttava siten, että siitä jää aukoton kirjausketju (audit trail). Tunnuksia sähköisesti jaettaessa on käytettävä vahvaa salausta.

Aalto-yliopistossa saattaa olla käytössä myös niin sanottuja jaettuja käyttäjätunnuksia ja ryhmätunnuksia. Tällöin pääsyoikeudet on sidottu tähän jaettuun käyttäjätunnukseen. ks. tämän dokumentin osio 2.4. Yhteiskäytössä olevat käyttäjätunnukset.

2.2 Ylläpitotunnukset

Järjestelmien ylläpitotehtävissä käytetään erillistä, ylläpitotehtäviin tarkoitettua henkilökohtaista tunnusta. Järjestelmävalvojan oikeuksilla varustettua tunnusta ei saa käyttää muiden päivittäisten töiden tekemiseen tai yksityiseen käyttöön, kuten sähköpostin tai internetin käyttöön.

Ylläpito-oikeuksia jaetaan käyttötarveperustaisesti. Toiminnoista vastaava tai hänen valtuuttamansa henkilö päättää ylläpito-oikeuksien myöntämisestä nimetyille henkilöille. Ylläpito-oikeudet myönnetään erillisille, ylläpitäjien omille ylläpitotunnuksille.

IT-palvelut pitää ylläpito-oikeuksista ja ylläpitohenkilöistä luetteloa. Toiminnoista vastaava vastaa siitä, että oikeudet on ilmoitettu luetteloon ja luettelo on ajan tasalla. Toiminnoista vastaava katselmoi yhdessä IT-palveluiden kanssa ylläpitotunnukset vuosikellon mukaisesti.

Suojattavalle kohteelle on IT-palveluiden määriteltävä ne roolit, jotka ovat tarpeen kohteen ylläpitotehtävien hoitamiseksi.

2.3 Tekniset ja palvelutunnukset

Teknisillä ja palvelutunnuksilla on omistaja, joka vastaa niiden dokumentoinnista. Omistajuus on kirjattu tietojärjestelmän dokumentaatioon.

2.4 Yhteiskäytössä olevat tunnukset

Yhteiskäytössä olevilla tunnuksilla tarkoitetaan ryhmätunnuksia ja jaettuja tunnuksia. Yhteiskäytössä olevien tunnusten luottamuksellisuutta on suojattava vaihtamalla salasana säännöllisesti ja aina tarvittaessa. Toiminnoista vastaava, tai hänen nimittämä henkilö, katselmoi yhdessä IT-palveluiden kanssa vastuualueeseensa liittyvien järjestelmien yhteiskäytössä olevat tunnukset vuosikellon mukaisesti.

2.4.1 Jaetut käyttäjätunnukset

Jaetut käyttäjätunnukset sallitaan vain erikoistilanteissa. Jaetut käyttäjätunnukset ovat sallittuja vain perustellusta syystä, esimerkiksi tutkimuskäyttöön. Suojattavan kohteen (esimerkiksi tietojärjestelmän) omistaja päättää jaetun tunnuksen käytöstä.

Henkilötietojen käsittely jaetuilla käyttäjätunnuksilla on kielletty. Henkilötiedoilla tarkoitetaan sellaisia tietoja, joiden perusteella henkilö tunnistetaan tai voidaan tunnistaa. Esimerkiksi nimi, ip-osoite ja auton rekisterinumero ovat henkilötietoja. Käsittelyllä taas tarkoitetaan esimerkiksi henkilötietojen keräämistä ja luovuttamista.

Luottamuksellisia tietoja käsiteltäessä on syytä huolehtia siitä, että kaikilla jaettuja tunnuksia käyttävillä on tarve ja oikeus päästä käsiksi kyseisiin tietoihin.

Jokainen jaettuja käyttäjätunnuksia käyttävä on vastuussa omalta osaltaan jaetuilla tunnuksilla tapahtuvasta käytöstä. Jaettuja käyttäjätunnuksia käytettäessä on erityisesti huomioitava se, että tietoturvan takaamiseksi salasana on erityisen tärkeää vaihtaa riittävän usein ja sen on oltava riittävän laadukas. Ks. tarkemmin salasanaohje.

2.4.2 Ryhmätunnukset

Ryhmätunnukset ovat määräaikaisia ja ne sallitaan vain erityisiin tarkoituksiin. Useamman henkilön käytössä olevia ryhmätunnuksia voidaan myöntää erityisiin tarkoituksiin, esimerkiksi kurssien käyttöön työasemaluokissa.

Ryhmätunnuksen anoja vastaa tunnuksen luovuttamisesta vain kyseiseen tarkoitukseen, esim. kurssin osallistujille. Ryhmätunnuksen käytön myöntää toiminnoista vastaava. Ryhmätunnusta saa käyttää vain siihen tarkoitukseen, johon se on myönnetty.

Ryhmätunnukset ovat määräaikaiset. Ryhmätunnukselle on sen luonnin yhteydessä asetettava elinkaari. Tunnus lukkiutuu määräajan päätyttyä.

Jokainen ryhmätunnuksen käyttäjä on vastuussa ryhmätunnuksen käytöstään. Ryhmätunnuksella ei saa käsitellä luottamuksellisia tietoja tai henkilötietoja. Ryhmätunnuksia käytettäessä tulee erityisesti huomioida tämän dokumentin osio ”salasanojen käyttö”.

3 Pääsyoikeuksien myöntäminen ja hallinta

a) **Pääsy perustuu kirjalliseen sopimukseen ja sitoumukseen noudattaa tietoturvaa ja tietosuojaa koskevia määräyksiä**
Pääsyoikeudet perustuvat palvelussuhteeseen henkilön ja Aalto-yliopiston välillä tai muuhun kirjalliseen sopimukseen henkilön ja

Aalto-yliopiston välillä. Pääsyoikeudet saanut henkilö sitoutuu kirjallisesti noudattamaan Aalto-yliopiston tietosuoja- ja tietoturvapolitiikkoja sekä sääntöjä, määräyksiä ja ohjeita. Henkilö on sitoutunut pitämään kirjautumiseen tarvittavat tiedot salassa ja olemaan käyttämättä niitä väärin.

b) Pääsy perustuu henkilön rooliin (roolipohjaisuus)
Pääsyoikeudet on ryhmitelty rooleihin ja ryhmiin, ja henkilöllä voi olla useita rooleja ja ryhmiä. Henkilön kuuluessa tiettyyn ryhmään, kuten opiskelijat, hänelle avataan oletusarvoisesti pääsy ryhmään kuuluviin järjestelmiin ja tietoihin. Nämä roolit ja ryhmät sekä niiden avaamat pääsyt on kuvattava ja toiminnoista vastaavan on hyväksyttävä menettely. Henkilön roolin muuttuessa tulee pääsyoikeuksia, niin pääsyoikeuksia fyysisiin tiloihin kuin järjestelmiinkin, muuttaa vastaavasti.

c) Pääsyoikeudesta päättää toiminnoista vastaava, mutta eri lähteistä tulevat vaatimukset on otettava huomioon
Toiminnoista vastaava päättää pääsyn myöntämisestä ja turvallisen kirjautumisen (monivaiheinen tunnistautuminen (MFA)) käytöstä. Pääsyoikeuksien myöntämisessä on otettava huomioon lainsäädännön, sopimusten sekä Aalto-yliopiston toimintaa koskevat vaatimukset ja erityisesti tarve suojata henkilötietoja ja muuta Aalto-yliopiston suojattavaa omaisuutta (esimerkiksi Aalto-yliopiston liikesalaisuudet).

d) Pääsyoikeudet myönnetään ensisijaisesti pääsyoikeuksien hallintajärjestelmän avulla
Lähtökohtaisesti pääsyoikeudet myönnetään, muutetaan ja kumotaan pääsyoikeuksien hallintajärjestelmän avulla. Tilanteissa, joissa pääsyoikeuksien hallintajärjestelmä tulee ohittaa ks. tämän dokumentin ensimmäisen luvun periaatteet.

- Järjestelmien käyttöoikeuksien hallintaan on nimetty toiminnoista vastaavan vastuuhenkilö, jos se ei ole toiminnoista vastaava.
- Järjestelmän käyttäjistä on olemassa ajantasainen lista.
- Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin, opiskeluun tai toimeksiantoon liittyviin verkkoihin, tietoihin ja järjestelmiin.
- Pääsyoikeuden myöntämisen yhteydessä tarkistetaan luotettavalla tavalla, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
- Pääsyoikeuksien käsittely ja myöntäminen on ohjeistettu kunkin järjestelmän osalta.

- On olemassa selkeä ja toimiva tapa henkilöstössä ja opiskelijakunnassa sekä yhteistyötahojen henkilökunnassa tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.
- Pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön.
- Pääsyoikeudet katselmoidaan säännöllisesti.
- Yhteistyökumppanien/muiden ulkopuolisten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä.
- Jokaisesta myönnetystä pääsyoikeudesta jää merkintä.

4 Käyttäjätunnuksen sekä pääsyoikeuksien luonti ja myöntäminen

4.1 Vaihe 1: Käyttäjätunnuksen luonti

Ennen käyttäjän rekisteröimistä ja käyttäjätunnuksen luontia on hänet tunnistettava vahvalla tunnistamismenetelmällä (sähköinen tunnistus tai passi/virallinen kuvalla varustettu henkilöllisyystodistus). Pelkkä käyttäjän rekisteröinti ja käyttäjätunnus eivät avaa pääsyä verkkoihin ja verkkopalveluihin. Pääsyoikeudet saanut henkilö sitoutuu kirjallisesti noudattamaan Aalto-yliopiston tietosuoja- ja tietoturvapolitiikkoja sekä sääntöjä, määräyksiä ja ohjeita.

4.2 Vaihe 2: Pääsyoikeuden myöntäminen

Rekisteröidylle käyttäjälle (käyttäjätunnukselle) sallitaan pääsy ainoastaan niihin verkkoihin ja verkkopalveluihin, joihin hänelle on nimenomaisesti myönnetty pääsyoikeudet. Pääsyoikeudet myönnetään lähtökohtaisesti rooliin perustuen, jos henkilöllä on jokin rooli Aalto-yliopistossa. Pääsyoikeuksien myöntämisessä huomioidaan kuitenkin vaatimukset tarpeesta tietää ja käyttää tietoa.

Pääsyoikeus Aalto-yliopiston tietojärjestelmiin alkaa työsuhteen alkamispäivänä. Perustellusta syystä käyttöoikeus voi alkaa 7 päivää ennen työsuhteen alkamista.

Opiskelijalle myönnetään opiskelussa tarvitsemiensa Aalto-yliopiston tietojärjestelmien käyttöoikeus, kun hänellä on voimassa oleva opintooikeus.

Muille tahoille käyttöoikeudet myönnetään tapauskohtaisesti huomioiden vaatimukset tarpeesta tietää ja tarpeesta käyttää. Tämä koskee esimerkiksi toimeksiantosuhteita.

5 Pääsyoikeuksien ja käyttäjätunnuksien poistaminen ja muuttaminen

Pääsyoikeus tietojärjestelmään poistetaan, kun
a) henkilö ei enää kuulu Aalto-yliopistoon
b) määräaikaiseksi myönnetty pääsyoikeus vanhenee

c) henkilön rooli muuttuu siten, ettei tietojärjestelmän pääsyoikeudelle enää ole perustetta
d) se on tarpeen tietoturvallisuuden vaarantumisen takia, esimerkiksi tietotekniikkarikkomuksen selvittämiseksi tai tietojen turvaamiseksi.

Käyttäjätunnus suljetaan, kun
a) pääsyoikeus, johon liittyen se on annettu, loppuu
b) tunnukselle ei enää ole tarvetta
c) on olemassa perusteltu epäily tunnuksen väärinkäytöstä tai tietoturvallisuuden vaarantumisesta

IT-peruspalveluiden pääsyoikeuden loppuessa sähköposti sulkeutuu samalla niin, ettei uutta sähköpostia oteta enää vastaan. Tästä tarkemmin katso sähköposti- ja pikaviestisääntö Aalto-yliopiston opiskelijoille ja sähköposti- ja pikaviestisääntö Aalto-yliopiston yksiköille ja henkilökunnalle.

5.1 Pääsyoikeuksien uudelleenarviointi ja muuttaminen

Toiminnoista vastaavan on IT-palveluiden kanssa uudelleenarvioitava pääsyoikeuksia säännöllisesti tietoturvallisuuden hallintajärjestelmän vuosikellon mukaan ja poistettava vanhentuneet ja tarpeettomat pääsyoikeudet. Ensisijaisesti tarvittavista poistoista ja muutoksista huolehtii henkilön esimies ja toissijaisesti toiminnoista vastaava, tai hänen valtuuttama henkilö, säännöllisillä vuosikellon mukaisilla käyttöoikeuksiin liittyvillä tarkoituksenmukaisuuskatselmoinneilla.

Mikäli kustakin pääsyoikeudesta järjestelmään maksetaan lisenssi- tai käyttäjämaksu, on toiminnoista vastaavan, tai hänen valtuuttamansa henkilön, säännöllisesti huolehdittava siitä, että vain henkilöillä, jotka tarvitsevat lisenssejä työtehtäviensä tai opintojensa hoitamiseen, on lisenssi kyseiseen järjestelmään.

5.2 Käytännön tilanteet, henkilökunta

Henkilökuntaan kuuluvan pääsyoikeus Aalto-yliopiston tietojärjestelmiin päättyy kahdeksan päivää työsuhteen päättymisen jälkeen (sopimuksen päättymispäivä). Tuntiopettajilla pääsyoikeus jatkuu sen lukukauden loppuun, jonka aikana tuntiopetusmääräys loppuu.

Henkilön tulee pyytää tunnushallintoa sulkemaan käyttäjätunnuksensa, mikäli hän ei käytä niitä esimerkiksi pitkän poissaolon aikana. Jos työntekijä lakkaa hoitamasta työtehtäviään jo ennen työsuhteen päättymistä (esimerkiksi lomalle jäämisen vuoksi), yksikkö voi ilmoittaa käyttäjätunnuksen sulkemisesta tunnushallintoon, kun työtehtävien suorittaminen tosiasiallisesti päättyy. Jos henkilön kanssa on sovittu, että hän hoitaa työsuhteen päättymisen jälkeen tiettyjä tehtäviä (esim. opintojen ohjaus), yksikkö voi ilmoittaa henkilön pääsyoi-

keuden jatkamisesta ilman työsuhdetta. Tällöin voi kuitenkin olla tarpeen tarkastella pääsyoikeuksien laajuutta uudelleen, sillä henkilön asema suhteessa Aalto-yliopistoon muuttuu.

5.3 Käytännön tilanteet, opiskelija

Opiskelijan valmistuessa pääsyoikeus on voimassa 4 kuukauden ajan valmistumispäivästä, ja poistetaan tämän jälkeen.

Tämän määräajan jälkeen opiskelija voi ainoastaan erittäin painavista syistä hakea jatkoaikaa. Jatkoaikapyyntö tulee esittää omaan opintotoimistoon. Tietyn ajan jälkeen pääsyoikeuden avaaminen ei ole enää mahdollista.

6 Käyttäjän vastuu

6.1 Käyttäjien tunnistautumistietojen jakaminen

Tunnistautumistiedot (käyttäjätunnus ja salasana) ovat henkilökohtaiset ja luottamukselliset, eikä niitä saa luovuttaa kenellekään muulle. Käyttäjä on vastuussa toimista ja tiedoista, jotka on tehty tai talletettu käyttäen hänen tunnistautumistietojaan.

6.2 Luottamuksellisuuden menettäminen

Käyttäjän on viipymättä ilmoitettava Aalto-yliopiston tietoturvatiimille (security(at)aalto.fi), jos hän epäilee tunnistautumistietonsa päätyneen ulkopuolisen haltuun.