Gradian tietoverkon ja tietojärjestelmien käyttösäännöt

1. JOHDANTO

Jyväskylän koulutuskuntayhtymä Gradian (myöhemmin Gradia) tietoverkon ja tietojärjestelmien käyttösäännöt sitovat Gradian opiskelijoita ja henkilökuntaa sekä kaikkia muita, jotka ovat saaneet oikeudet Gradian tietojärjestelmien ja tietoverkon käyttöön.

Gradian tehtävänä on tarjota hyvä ja luotettava tietoverkko ja tietojärjestelmät takaamaan käyttäjilleen niiden turvallisen ja joustavan käytön. Tavoitteena on säilyttää tietojen luottamuksellisuus, eheys ja käytettävyys.

Tämä edellyttää käyttäjiltään vastuuntuntoa ja velvollisuuksiensa noudattamista sekä näiden käyttösääntöjen hyväksyntää. Tahatonkin käyttösääntöjen vastainen käyttö voi vaarantaa edellä mainittujen seikkojen toteutumisen.

2. KÄYTTÖSÄÄNNÖT JA KÄYTÖN PERIAATTEET

Näitä sääntöjä ja muita Gradian ohjeita koskien mm. tietoturvaa ja tietosuojaa on kaikkien käyttäjien noudatettava. Sääntöjen piiriin kuuluvat kaikki Gradian ja Gradian hankkeiden kautta hankkimat työasemat, tietotekniikkapalvelut, tietojärjestelmät ja tietoverkkoon liitetyt laitteet. Lisäksi käyttösääntöjä on noudatettava kaikissa muissa palveluissa ja tietoverkoissa, joihin käyttäjä on saanut käyttöluvan ja käyttömahdollisuuden Gradian välityksellä. Käyttösäännöt koskevat myös Gradiassa käytettäviä ja Gradian verkkoa hyödyntäviä omia laitteita.

3. KÄYTTÖOIKEUS

Käyttöoikeus syntyy hyväksymällä nämä käyttösäännöt. Sääntöjen hyväksyminen tapahtuu sähköisesti. Käyttöoikeudet määritetään henkilön tehtävän mukaan.

Järjestelmillä, laitteilla ja tietoverkolla voi olla Gradian laatimia erillisiä ohjeita, joihin käyttäjän tulee tutustua ennen niiden käyttöä.

4. KÄYTTÄJÄTUNNUKSET

Käyttäjä vastaa saamistaan käyttäjätunnuksista, niiden salasanoista ja huolehtii salasanojen vaihtamisesta ilmoitettujen ohjeiden mukaisesti. Käyttäjätunnuksia ja salasanoja ei saa luovuttaa toiselle henkilölle. Työaseman jäädessä ilman käyttäjän valvontaa, on käyttäjän kirjauduttava ulos tai lukittava kone estääkseen työaseman luvattoman käytön.

5. KÄYTTÖOIKEUDEN VOIMASSAOLO

Käyttöoikeus on voimassa palvelussuhteen tai opiskelun alkamisesta sen päättymiseen asti. Mikäli käyttöoikeus on syntynyt muun sopimuksellisen perusteen nojalla, käyttöoikeus päättyy sopimuksen päättyessä. Käyttöoikeus tietyn järjestelmän tai resurssin osalta voi muuttua tai päättyä, mikäli käyttäjän tehtävä muuttuu.

Käyttäjän on itse huolehdittava ennen käyttöoikeuden päättymistä omistuksessaan olevien tietojen siirroista ja poistoista. Käyttäjän tunnus lukittuu automaattisesti 14 vrk käyttöoikeuden päättymisen jälkeen. Opiskelijoiden tiedostot ja sähköpostit poistetaan 90 päivän kuluttua ja henkilökunnan 180 päivän kuluttua tunnuksen lukittumisesta, eikä tietoja ole mahdollista palauttaa tämän jälkeen.

6. KÄYTTÖRAJOITUKSET

Gradian tietoverkon, tietojärjestelmien ja käyttäjätunnusten käyttö poliittiseen tai Gradialle kuulumattomaan kaupalliseen toimintaan on kielletty. Tutkimustoimintaan tarvitaan lupa. Yksityinen käyttö on kohtuullisessa määrin sallittua, mutta ei saa häiritä Gradian normaalia toimintaa. Yksityiset tiedot tulee pitää erillään Gradian aineistosta. Henkilökunnan tulee sijoittaa yksityinen aineistonsa kotihakemiston (H-asema) tai OneDriven yksityisiin kansioihin. Ohje koskee myös yksityisluonteista sähköpostia, jotka on sijoitettava erillisiin sähköpostikansioihin. Yksityiset aineistot tulisi voida erottaa kansion nimestä (esim. private, yksityisasiat).

Kaikki lain mukaan salassa pidettävä aineisto[1] on sijoitettava Gradian verkkolevyille tai Gradian tietojärjestelmiin. Gradian OneDrive- tai Sharepoint-ympäristöä voi käyttää tiedon tallennukseen kuten verkkolevyasemia. Julkisten tai yksityiskäytössä olevien pilvipalveluiden, suojaamattomien muistitikkujen ja ulkoisten kovalevyjen käyttö salassa pidettävän aineiston tallennukseen on kielletty. Henkilötietoja sisältävät tiedot on kuitenkin sijoitettava pääosin edelleen niille varattuihin tietojärjestelmiin tai työn kannalta oikeutettujen henkilöiden käyttäjätunnuksilla suojattuihin kansioihin verkkolevyasemille.

Omille ja vierailijoiden laitteille on varattu langaton verkko. Kaikenlainen Gradian tietoteknisten laitteiden kytkentöjen muuttaminen ja vahingoittaminen, tietoverkon tai tietojärjestelmien häirintä tai toiminnan estäminen on kiellettyä.

Vastuu tietoaineistojen säilymisestä on viime kädessä aineiston omistajalla itsellään. Gradia ei korvaa käyttäjälle aiheutunutta vahinkoa tai menetystä, joka johtuu Gradian tietojärjestelmien tai tietoverkon käytöstä.

7. TIETOSUOJA

Tietosuojassa on kyse ihmisten yksityiselämän suojan ja muiden yksityisyyden suojaa turvaavien perusoikeuksien toteuttamisesta henkilötietojen käsittelyssä. Tietosuojaan tulee kiinnittää erityistä huomiota ja vahingossakin saadun muille kuuluvan tiedon tallentaminen, hyväksi käyttäminen tai jakaminen on kiellettyä.

[1] **Salassa pidettävä aineisto** = Julkisuus- ja salassapitosäädösten mukaisesti salaiseksi määritelty aineisto, kuten esim. terveydentilatiedot, perhe-elämää ja henkilökohtaisia oloja, opiskeluhuoltoa ja opiskelijan opetuksesta vapauttamista koskevat tiedot, psykologiset testit ja soveltuvuuskokeet sekä mm. henkilön salaiseksi ilmoittamat yhteys- ja sijaintitiedot.

Kaikenlainen oikeudeton tiedon hankkiminen sekä hakemistoihin, tietoverkkoihin tai tietojärjestelmiin tunkeutumisen yrittäminenkin on kielletty.

8. LUVATON TAI MUU VÄÄRINKÄYTTÖ

Henkilö, joka toimii yleistä lainsäädäntöä tai näitä käyttösääntöjä vastaan tai jota voidaan perustellusti epäillä tietoturvallisuuden tai tietosuojan rikkomisesta, voi menettää käyttöoikeutensa tai sitä voidaan rajoittaa. Kyseeseen voi tulla myös huomautus, varoitus, korvauksen periminen tai asia voidaan antaa poliisin tutkittavaksi.

9. YLLÄPITO JA VALVONTA

Kullakin tietojärjestelmällä on omistaja ja pääkäyttäjä, jotka vastaavat järjestelmän käytöstä ja sen käyttöohjeiden laadinnasta. Laitteista, tietoverkosta ja tietojärjestelmistä vastaa Gradian Digipalvelut lukuun ottamatta tietojärjestelmiä, jotka on hankittu kolmannen osapuolen toimittamina palveluina tai on muutoin ulkoistettu. Gradian yksiköiden omassa valvonnassa olevista laitteista tai teknisistä ympäristöistä vastaa yksikkö itse.

Gradian Digipalveluiden ylläpitohenkilökunnalla on velvollisuuksiensa hoitamiseksi lupa valvoa (lokitiedot), rajoittaa ja säädellä tietojärjestelmien ja tietoliikenneverkon käyttöä sekä tarvittaessa kopioida, siirtää, poistaa koneissa tai verkossa olevaa tietoa.

Nämä käyttösäännöt on käsitelty Gradian henkilöstön osalta yhteistoimintalain mukaisesti. Näitä sääntöjä päivitetään tarvittaessa Gradian palveluissa tai lainsäädännössä tapahtuneiden muutosten vuoksi. Päivityksestä vastaa ja sen tarvetta seuraa vuosittain digipalvelupäällikkö sekä tietosuoja- ja tietoturvavastaavat. Viimeisin versio julkaistaan Gradian intranetissä sekä Gradian julkisilla verkkosivuilla www.gradia.fi. Vikailmoitukset, väärinkäytökset ja tiedustelut tulee osoittaa sähköpostilla digipalvelut@gradia.fi tai soittamalla numeroon 040 341 5123.

Vahvistettu kuntayhtymän johtajan päätöksellä 12.6.2018.

Rules of use for Gradia's information network and information systems

1. INTRODUCTION

Rules of use for the information network and information systems of Jyväskylä Educational Consortium Gradia (hereinafter Gradia) apply to Gradia's students and staff as well as all others who have received the right to use Gradia's information systems and information network.

Gradia's duty is to offer a fluently operating, reliable information network and information systems to guarantee their safe and flexible use. The aim is to maintain the confidentiality, integrity and accessibility of the information.

This requires a sense of responsibility and the fulfilment of obligations from the users as well as the approval of these rules of use. Even unintentional use against the rules of use can endanger the fulfilment of the above requirements.

2. RULES OF USE AND PRINCIPLES OF USE

All users must follow these rules and Gradia's other instructions concerning, for example, information security and data protection. The rules cover all workstations, IT services, information systems, and network-connected equipment acquired through Gradian and Gradian projects. In addition, these rules of use must be followed in all other services and information networks for which the user has received the right and possibility of use via Gradia. The rules of use also apply to equipment used in Gradia or making use of Gradia's network.

3. RIGHT OF USE

A right of use is established with the approval of these rules of use. The rules are approved electronically. The rights of use are determined according to the person's tasks.

There can be separate instructions prepared by Gradia for systems, equipment and the information network, which the user should become familiar with before their use.

4. USER IDS

The user is responsible for the user IDs and passwords he/she has received as well as replacing the passwords according to the instructions given. User IDs and passwords may not be disclosed to another person. When the workstation is left unattended, the user must log out or lock the computer to prevent the unauthorised use of the workstation.

5. VALIDITY OF THE RIGHT OF USE

The right of use remains valid throughout of the employment relationship or studies. If the right of use is based on some other contractual ground, it will end when the agreement ends. The right of use to a specific system or resource may change or end if the user's task changes.

The user must personally take care of the transfer and deletion of information in their possession before the expiry of the right of use. The user ID is locked automatically 14 days after the expiry of the right of use. Students' files and e-mails are deleted 90 days and those of the staff 180 days after the locking of the user ID, and the data cannot be recovered after that.

6. LIMITATIONS OF USE

The use of Gradia's information network, information systems and user IDs for political purposes or for commercial activities not belonging to Gradia is prohibited. A permit is required for research activities. Moderate private use is permitted, provided that it does not disturb Gradia's normal operations. Private information must be kept separate from Gradia's materials. The staff must place their private materials in the private folders of the home directory (H drive) or OneDrive. This also applies to e-mail of a private nature, which must be placed in separate e-mail folders. It should be possible to identify private materials from the name of the folder (e.g. private, private matters).

According to the law, confidential material[1] must be placed on Gradia's online disk storages or in Gradia's information systems. Gradia's OneDrive or Sharepoint environment can be used for saving information in the same way as online disk storage drives. The use of public or privately used cloud services, unprotected flash drives and external hard disks for saving confidential material is prohibited. However, materials containing personal data must still mainly be placed in information systems set aside for them or in folders on online disk storage drives that are protected with the user IDs of people authorised to access the data in their work.

A wireless network is available for Gradia's own and visitors' devices. Any change or damage to the connections of Gradia's IT equipment, disturbance of the information network or information systems or preventing the operation is prohibited.

Responsibility for the preservation of data sets ultimately lies with their owner. Gradia does not compensate any damage or loss incurred by the user that is due to the use of Gradia's information systems or information network.

7. DATA PROTECTION

Data protection involves protecting people's private lives and other fundamental rights safeguarding privacy protection in the processing of personal data. Special attention must be paid to data protection, and even the accidental saving, utilisation and distribution of data belonging to others is prohibited.

All unauthorised acquisition of data as well as attempting to access directories, information networks or information systems is prohibited.

8. UNAUTHORISED USE OR OTHER MISUSE

A person who violates general legislation or these rules of use or who can be justifiably suspected of violating information security or data protection can lose their right of use or it can be limited. The person may also be given a warning, become liable to pay compensation or the matter may be subjected to police investigation.

9. MAINTENANCE AND SUPERVISION

Each information system has an owner and administrator, who are responsible for the use of the system and for preparing instructions for it. Gradia digital services is responsible for the equipment, information network and information systems, except for information systems acquired as a service from a third party or otherwise outsourced. Each unit is responsible for equipment or technical environments under the supervision of Gradia's units.

The administration staff of Gradia digital services have the permission to supervise (log data), limit and regulate the use of information systems and the telecommunications network and, where necessary, to copy, transfer and delete data in computers or the network in order to fulfil their obligations.

These rules of use have been discussed according to the Act on Co-operation within Undertakings for Gradia's personnel. Where necessary, these rules will be updated according to changes taking place in Gradia's services or legislation. The digital service manager and information security and data protection officers are responsible for the update and monitoring the need for the update. The most recent version is published in the Gradia intranet and on Gradia's public website www.gradia.fi. Fault reports, notifications of misuse and inquiries must be submitted by e-mail to digipalvelut@gradia.fi +358 40 341 5123.

Confirmed by administrative decision of the CEO of Jyväskylä Educational Consortium, 12 June 2018.