Käyttövaltuusperiaatteet

Tämä dokumentti kuvaa Itä-Suomen yliopiston ylioppilaskunnan (ISYY) käyttövaltuushallinnan yleiset periaatteet.

Identiteetin hallinta

Periaate 1: Tietojärjestelmiä käyttävät henkilöt pitää tunnistaa.

1. Perustettaessa uusi käyttäjätunnus ISYYn sähköiseen käyttöympäristöön tehdään ensimmäinen tunnistus käyttäjän täyttämän henkilötietolomakkeen perusteella.
2. Henkilöiden pitää olla hyväksyttyjä käyttämään ISYYn käyttöympäristöä työsuhteen tai sitä vastaavan muun sopimuksen taikka luottamushenkilöaseman perusteella.
3. Henkilötunnusta voi käyttää henkilöiden erottamiseen toisistaan järjestelmän sisällä.

Periaate 2. Käyttäjätunnukset ovat henkilökohtaisia

1. Yhteiskäyttöisiä käyttäjätunnuksia ei perusteta eikä niitä saa käyttää.
2. Käyttäjätunnus voidaan jäljittää luotettavasti henkilöön.
3. Käyttäjätunnuksiin ja laajemmin henkilöiden sähköisiin identiteetteihin liittyvät tiedot pidetään ajan tasalla.
4. Tietojärjestelmissä pidetään yllä käyttäjärekisteriä.

Käyttöoikeuksien hallinta

Periaate 3. Käyttöoikeuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu.

1. Käyttöoikeudet ovat henkilö- tai tehtäväroolikohtaisia.
2. Käyttöoikeuksien hallintaan on sovittu prosessi.
3. Käyttöoikeudet myönnetään silloin, kun työtehtävät niin edellyttävät.
4. Käyttöoikeudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.
5. Ylläpito-, pääkäyttäjä- ja hallintaoikeuksista ja niihin liittyvistä tehtävistä ohjeistetaan erillisellä määräyksellä tietojärjestelmien ylläpidosta.

Periaate 4. Tietojärjestelmien käyttäjätunnukset ja käyttöoikeudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja oikeudet suljetaan tai poistetaan.

1. Työroolien tai -tehtävien muuttuessa käyttöoikeudet pitää katselmoida ja tarvittaessa muuttaa vastaamaan tarpeita. Muutokset voivat johtua esimerkiksi lainsäädännöstä, joka edellyttää tietyissä työtehtävissä laajempia tai suppeampia käyttöoikeuksia tietoihin.
2. Käyttäjän ja esimiehen tulee yhteistyössä huolehtia siitä, että käyttöoikeudet päätetään silloin, kun työtehtävät eivät enää edellytä kyseisen tietojärjestelmän sisältämien tietojen käyttöä.

Käytönvalvonta

Periaate 5.: Tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytönvalvonnan sekä tietoverkkojen ja tietojärjestelmien asianmukaisilla ja riittävillä turvallisuusjärjestelyillä.

1. Yksittäisen käyttäjän käyttöoikeudet voidaan selvittää tarvittaessa myös jälkikäteisesti.
2. Käyttöoikeuksien myöntöprosessista pitää jäädä jälki (lokitieto tai dokumentti), milloin ja millä perusteella käyttäjälle on myönnetty käyttöoikeus ja kuka sen on myöntänyt.
3. Käyttöoikeuksien muutosprosessista pitää jäädä jälki (lokitieto tai dokumentti), milloin ja millä perusteella käyttöoikeuksia on muutettu tai ne ovat poistettu ja kuka muutokset on tehnyt.
4. Järjestelmien tuottamiin käyttölokitietoihin saa olla pääsy ainoastaan henkilöillä, joiden työtehtäviin käyttölokien valvonta tai muu käsittely on sovittu.

Periaate 6. Käytön seurantaan ja valvontaan on laadittu kirjallinen suunnitelma, jota noudatetaan.

1. Käyttäjätunnusten (aktiivisten ja passiivisten) määrää seurataan ja siltä osin kuin kustannuksia aiheutuu tunnuspohjaisesti, tilastoidaan myös niistä aiheutuvia kustannuksia (esimerkiksi lisenssimaksuja).
2. Ylläpito-, pääkäyttäjä- ja hallintaoikeuksien määrää ja käyttöä kontrolloidaan tarkasti.

Tietoturva ja tietosuoja

Periaate 7. Tietojärjestelmien tietoturva- ja tietosuoja-asioista huolehtiminen muodostuu osaksi toimintakulttuuria.

1. Noudatetaan organisaation tietoturvapolitiikkaa, johon jokaisen tietojärjestelmiä tai tietoja käyttävän pitää perehtyä.
2. Organisaation salassa pidettävien tietojen käyttäjiltä edellytetään ajanmukaisen tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen hyväksyminen.
3. Tietojärjestelmissä käsiteltävien tietojen salassapito ja muu suoja varmistetaan antamalla käyttöoikeudet tarvittavassa laajuudessa vain niille henkilöille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekistereihin talletettuja henkilötietoja työtehtäviensä hoitamiseksi.
4. Kunnioitetaan työkavereiden sekä kansalaisten yksityisyyden suojaa.

5. Tietojärjestelmien ja tietojen väärinkäyttöön liittyviin epäilyihin luodaan ilmoituskanava/prosessi ja niihin reagoidaan nopeasti
6. Havaituista tietoturvallisuuden tai tietosuojan puutteista ja väärinkäytöksistä ilmoitetaan viivytyksettä järjestelmän vastuuhenkilöille tai tietosuojavastaavalle.
7. Ymmärretään imagolliset asiat sekä se, että vahingon torjunta on halvempaa kuin sen korjaaminen.

Periaate 8. Teknisestä tietoturvasta huolehditaan suunnittelemalla ja toteuttamalla tietojärjestelmäratkaisut huolellisesti.

1. Tietojärjestelmähankinnoissa pitää pakollisilla vaatimuksilla huolehtia riittävän korkeasta tietoturvatasosta ja noudattaa Eu:n tietosuoja-asetuksen periaatetta ”privacy by default” Huomionarvoisia asioita ovat mm. tunnistautuminen, istunnon hallinta, käyttövaltuuksien hallinta ja tietojen suojaus. Tietojen tai toiminnan osalta kriittiset järjestelmät tulee auditoida tarpeen vaatiessa ja mieluiten ensimmäisen kerran ennen käyttöönottoa.
2. Tietojärjestelmien salasanoja ei tallenneta eikä välitetä verkon yli selväkielisenä. Esimerkiksi www-pohjaisissa sovelluksissa pitää sisään kirjautuminen tehdä käyttäen salattua yhteyttä (yleensä https-protokollaa).

Periaate 9. Tietojärjestelmien käyttöön, tietoturvaan ja salassapitoon liittyvät asiat perehdytetään käyttäjille.

1. Yleisen perehdytyksen yhteydessä on tietojen ja tietojärjestelmien käyttöoikeuksiin ja käyttöön liittyvät asiat perehdytettävä.
2. Työntekijät perehdytetään siihen, että he vastaavat käyttäjätunnuksiensa huolellisesta käytöstä ja että he eivät saa antaa käyttäjätunnustaan/salasanaansa toisen henkilön käyttöön.
3. Henkilöstölle annetaan ohjeet ja koulutusta sähköisten asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä. Annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.