Laki julkisen hallinnon tiedonhallinnasta, luonnos 13.10.2020 Suosituskortti	B
16 § Käyttöoikeuksien hallinta	versio 0.9

16 § Tietojärjestelmien käyttöoikeuksien hallinta

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina.

Perustelumuistio
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Asianmukaisen pääsynhallinnan ja käyttäjienhallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä.

Ainoastaan valtuutetuille käyttäjille sekä järjestelmille myönnetään pääsy- ja käyttöoikeustietoihin ja tietojärjestelmiin. Käyttöoikeuksien hallinnan tulee noudattaa vähimpien oikeuksien periaatetta ja sen on katettava järjestelmien koko elinkaari. Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työn suorittamiseksi välttämättömiä. Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi.

Käyttöoikeuksien hallinnan edellytykset

1) Käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2) Käyttäjätilien luontiin, hyväksymiseen, ylläpitoon ja poistamiseen tulee olla ennalta määritelty prosessi ja käyttöoikeus tulee perustua tunnuksen saajan kanssa tehtyyn sopimukseen (Esim. työsopimus, ostopalvelusopimus)
3) Järjestelmien käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä. Tunnuksen omistajuus on määriteltävä erikseen jos myönnetään tunnuksia konetileille esim. ohjelmistorobotiikan käyttöön.
4) Järjestelmän käyttäjistä tulee ylläpitää listaa. Jokaisesta myönnetystä käyttöoikeudesta tulee jäädä merkintä (paperi tai sähköinen). Myös kaikista muutoksista on jäätävä merkintä.
5) Käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu ja että henkilöllä on riittävä koulutus kulloisenkin järjestelmän käyttöön.
6) Organisaation ulkoiset ja sisäiset käyttäjät tulisi olla eroteltavissa käyttäjätunnuksen perusteella.
7) Käyttöoikeuksien käsittely ja myöntäminen tulee ohjeistaa.
8) Tarpeettomat käyttäjätilit sekä tarpeettomat käyttöoikeudet ja -valtuudet tulee poistaa, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta, vaihtaessa työtehtäviään tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan).
9) Organisaatiolla on oltava selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa näistä johtuvien tarvittavien muutosten tekemiseen.
10) Käyttöoikeudet ja -valtuudet tulee katselmoida säännöllisesti. Katselmointi tulisi olla auditoitavissa esimerkiksi pöytäkirjasta.
11) Käyttöoikeudet on määriteltävä ennalta kullekin tietojärjestelmän käyttäjälle, heidän tyypillisten työtehtävien perusteella ja vähimpien oikeuksien periaatetta noudattaen (*Principle of Least Privilege*). Yhteiskäyttötunnuksia ei tulisi käyttää kuin erikseen hyväksytyissä poikkeustapauksissa.
12) Vaaralliset käyttövaltuusyhdistelmät on tunnistettava, dokumentoitava ja eriytettävä mahdollisuuksien mukaan (*Separation of Duties, SoD*). Mikäli tehtäviä ei voida eriyttää, tulee

niistä syntyviä riskejä hallita riskienhallinnan keinoin. Vaarallinen työyhdistelmä on kyseessä, jos henkilö käsittelee yksin väärinkäytös- ja virhealttiissa prosessissa koko tapahtumaketjun tai useampia sen osia.

13) Käyttöoikeuksien hallinnassa tulee kiinnittää huomiota etenkin korkeamman riskiprofiilin omaaviin työrooleihin (kuten pääkäyttäjät ja ylläpitäjät sekä muut erityistä luotettavuutta edellyttävät työtehtävät) ja niihin liitettyihin käyttöoikeuksiin ja -valtuuksiin. Erityistunnuksilla tulisi olla oma erillinen haku- ja päätösprosessi, jonka avulla määritetään toiminnan oikeellisuus.

Viranomaista suositellaan dokumentoimaan ja jalkauttamaan riskienarvioinnin pohjalta johdettu käyttövaltuuksien hallintapolitiikka. Politiikassa määritellään käyttövaltuuksien periaatteet ja toimintatavat. Tiedonhallintalain ja käyttövaltuuksien hallintapolitiikan lisäksi voimassa oleva tietosuojalainsäädäntö on otettava huomioon käyttöoikeuksien hallinnassa, koska henkilötietojen käsittely on olennainen osa käyttövaltuuksien hallintaa.

Muutosten hallinta

Muutosten yhteydessä (mm. ylennykset, alennukset, työnkierto, ja erityisesti työsuhteen päättyminen) oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Muutos voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan muutettua tarvittavana ajankohtana. Tämä voi tapahtua siten, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

Valvonta/Monitorointi:

Käyttäjätilejä, käyttöoikeuksia ja käyttövaltuuksia seurataan ja niiden käyttöä valvotaan dokumentoidusti asianmukaisuuden varmistamiseksi ja poikkeamien havaitsemiseksi. Valvonnan avulla seurataan, että käyttäjätilit, käyttöoikeudet ja käyttövaltuudet ovat ajan tasalla, ja niiden käyttö on asianmukaista ja noudattaa sovittuja käytäntöjä. Käyttöoikeuksien ja -valtuuksien käyttöä valvotaan käyttäjien normaalikäytöstä eroavien poikkeamien havaitsemiseksi ja niihin reagoimiseksi määritettyjen periaatteiden mukaisesti. Valvonnassa kiinnitetään huomiota etenkin erityistä luotettavuutta edellyttävien työtehtävien oikeuksien asianmukaisuuteen, ajantasaisuuteen ja käyttöön.

Kaikista käyttöoikeuksiin tehtävistä muutoksista ja oikeuksien käytöstä on jäätävä lokimerkintä. Lokitiedoista kerrotaan tarkemmin lokienhallintaa koskevassa kortissa [Kortti 17 § lokitietojen kerääminen].

Tunnistaminen ja todennus

Luotaessa uusi käyttäjätunnus järjestelmään, joka sisältää salassa pidettävää tietoa, tehdään ensimmäinen tunnistus valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen vahvaa tunnistusmenetelmää. Lisäksi käyttäjätunnusta luovutettaessa varmistutaan, että oikea henkilö saa käyttäjätunnuksen.

Kertakirjautumista (SSO) suositellaan käytettävän mahdollisimman laajasti. Kertakirjautumisella tarkoitetaan pääsynvalvonnan toteutustapaa, jossa yhdellä tunnistautumisella pääsee kaikkiin saman

pääsynvalvonnan piirissä oleviin palveluihin ja järjestelmiin, omien käyttöoikeuksien rajoissa. Kertakirjautuminen vähentää riskiä saman salasanan käytöstä useassa eri palvelussa tai salasanan uudelleen käyttämisestä.

Kertakirjautumisen lisäksi monivaiheista tunnistautumista (*Multifactor Authentication, MFA*) suositellaan käytettäväksi. Monivaiheisessa tunnistautumisessa käytetään kahta tai useampaa tunnistautumismenetelmää. Monivaiheisen tunnistautumisen avulla voidaan paremmin ehkäistä mahdollisia tietomurtoja.

Salasanoille on määritettävä riittävät laatuvaatimukset, esimerkiksi salasanan vähimmäispituus ja kompleksisuus. Laatuvaatimusten tulisi olla teknisesti pakotettuja.

Käyttäjä: organisaation työntekijä (sisäinen-ulkoinen), harjoittelija, opiskelija, asiakas tai organisaationsa toimintaan muulla tavoin liittyvä henkilö (esim. luottamushenkilö), joka käyttää palveluntarjoajien tarjoamia palveluja

Käyttäjärooli: joukko käyttäjän ominaisuuksia, jotka liittyvät hänen tietotarpeittensa ja/tai toimintavaltuuksiensa määrittelyyn Käyttäjäroolia voidaan katsoa joko käyttäjän toimenkuvan näkökulmasta (työrooli) tai hänellä palvelujärjestelmissä olevien valtuuksien näkökulmasta (ITrooli).

Käyttöoikeus, Käyttövaltuudet: tietojärjestelmän käyttäjälle tai esimerkiksi tietyn käyttäjäroolin omaavalle käyttäjäryhmälle myönnetyt yksilöidyt oikeudet nimettyjen palveluelementtien tai muiden resurssien käyttöön. Käyttövaltuudet määrittelevät, miten ja millaisilla edellytyksillä käyttäjällä on oikeus käyttää ao. palveluelementtejä.

Laajemmin eri termejä määritellään kansallisessa käyttövaltuushallinnan viitearkkitehtuurin liitteessä 5

Työkaluja:
Käyttövaltuushallintajärjestelmä (IAM), keskitetty tietojärjestelmä, jolla voidaan toteuttaa ja automatisoida identiteetti- ja käyttövaltuushallintaa ja sen valvontaa

Lisätietolähteitä:

- KATAKRI Auditointityökalu (https://www.defmin.fi/katakri)
- Kyberturvallisuuskeskuksen ohjeet (https://www.kyberturvallisuuskeskus.fi/fi/ohjeet)
- Microsoftin parhaat käytännöt (https://azure.microsoft.com/en-us/resources/security-best-practices-for-azure-solutions/)
- Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri (https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntasektorin%20k%C3%A4ytt%C3%B6valtuushallinnan%20viitearkkitehtuuri.pdf)