

1. Tarkoitus ja soveltamisala

Tämä ohjeistus kuvaa, miten kunkin järjestelmän RBAC-matriisia (roolipohjaista käyttövaltuusmatriisia, Role-Based Access Control) ylläpidetään sen elinkaaren aikana, kuka siitä vastaa, ja miten yksittäiset järjestelmäkohtaiset matriisit muodostavat yhdessä organisaation kokonaiskuvan käyttövaltuuksista.

Ohjeistus täydentää erillistä muokattavaa RBAC-matriisilomaketta, jota käytetään itse matriisien sisällölliseen dokumentointiin. Tätä ohjeistusta sovelletaan yrityksen kaikkiin järjestelmiin, joille on laadittu tai laaditaan RBAC-matriisi, riippumatta järjestelmän koosta tai kriittisyydestä.

2. Roolit ja vastuut

Käyttövaltuusmatriisin ylläpito on jaettu usean toimijan kesken. Alla oleva taulukko kuvaa keskeiset roolit ja niiden vastuut matriisin elinkaaren aikana.

Rooli	Vastuu
Järjestelmän omistaja (System Owner)	Vastaa oman järjestelmänsä RBAC-matriisin sisällöllisestä oikeellisuudesta. Määrittelee ja hyväksyy roolit ja niiden oikeudet, käynnistää katselmoinnit ja päivitykset sekä allekirjoittaa matriisin hyväksynnän.
Tietoturva / käyttövaltuushallinta	Ylläpitää matriisimallia ja -pohjaa, kokoaa järjestelmäkohtaiset matriisit organisaatiotason kokonaiskuvaksi, valvoo RBAC-standardin noudattamista sekä raportoi havaitut riskit ja poikkeamat.
Pääkäyttäjät / järjestelmävastaavat	Toteuttavat matriisissa määritellyt oikeudet käytännössä kohdejärjestelmään sekä ilmoittavat havaitsemistaan poikkeamista järjestelmän omistajalle.
HR / henkilöstöhallinto	Tuottaa tiedon roolimutoksista sekä aloittavista ja lähtevistä työntekijöistä matriisin ylläpidon ja käyttäjä-rooli-liitosten pohjaksi.
Sisäinen tarkastus / auditointi	Tarkastaa määräajoin, että järjestelmiin toteutuneet käyttöoikeudet vastaavat kulloinkin voimassa olevaa matriisia, ja raportoi poikkeamat.

3. Matriisin elinkaari

3.1 Luonti

Järjestelmän omistaja vastaa matriisin ensimmäisestä laadinnasta yhdessä pääkäyttäjien kanssa. Matriisiin kirjataan järjestelmän kaikki keskeiset roolit sekä moduulit/kohteet, ja jokaiselle roolin ja moduulin yhdistelmälle määritellään oikeudet (C, R, U, D tai ei pääsyä) RBAC-lomakkeen mukaisesti.

3.2 Katselmointi

Matriisi katselmoidaan säännöllisin väliajoin sekä aina merkittävän muutoksen yhteydessä. Katselmointiväli suositellaan sidottavaksi järjestelmän kriittisyyteen:

Järjestelmän kriittisyys	Suositteltu katselmointiväli
Kriittinen (esim. talous-, henkilöstö- tai asiakastietojärjestelmät)	2 kertaa vuodessa
Merkittävä	Kerran vuodessa
Matala	Joka toinen vuosi tai tarpeen mukaan

3.3 Muutoksenhallinta

Matriisia päivitetään aina kun järjestelmän rooleissa, moduuleissa tai niiden oikeuksissa tapahtuu muutoksia. Muutokset kirjataan matriisin muutoslokiin (versio, päivämäärä, tekijä, muutoksen kuvaus).

3.4 Hyväksyntä

Jokainen päivitetty matriisi hyväksytetään järjestelmän omistajalla. Tietoturva/käyttövaltuushallinta tarkastaa, että matriisi noudattaa RBAC-standardia ja vähimpien oikeuksien periaatetta ennen arkistointia.

3.5 Arkistointi ja versiohistoria

Hyväksytty matriisi arkistoidaan keskitettyyn, pääsynhallittuun sijaintiin. Jokainen versio säilytetään jäljitettävyyden vuoksi; aiempia versioita ei poisteta vaan korvataan uudella versionumerolla.

4. Milloin matriisi on päivitettävä

Seuraavat tilanteet laukaisevat tarpeen päivittää järjestelmän RBAC-matriisi:

- Uusi järjestelmä tai moduuli otetaan käyttöön.
- Uusi rooli perustetaan tai olemassa oleva rooli poistuu käytöstä.
- Organisaatiomuutos, joka vaikuttaa tiimien tai henkilöiden vastuisiin.
- Merkittävä prosessimuutos, joka vaikuttaa käyttöoikeustarpeisiin.
- Auditoinnissa tai tietoturvapöytätyössä havaittu puute tai virhe.
- Kalenterin mukainen määräaika-katselmointi (ks. kohta 3.2).

5. Yksittäisistä matriiseista kokonaisuudeksi

Järjestelmäkohtaiset matriisit eivät ole erillisiä dokumentteja vaan osa organisaation käyttövaltuushallinnan kokonaiskuvaa. Kokonaisuus muodostetaan seuraavien periaatteiden mukaisesti:

5.1 Keskitetty matriisirekisteri

Tietoturva/käyttövaltuushallinta ylläpitää keskitettyä rekisteriä (master inventory) kaikista järjestelmistä, joilla on RBAC-matriisi. Rekisteriin kirjataan vähintään järjestelmän nimi, omistaja, matriisin versio, viimeisin katselmointipäivä ja seuraava suunniteltu katselmointi.

5.2 Roolinimikkeiden yhdenmukaistaminen

Samantyyppiset roolit eri järjestelmissä nimetään mahdollisimman johdonmukaisesti (esim. "Pääkäyttäjä", "Peruskäyttäjä", "Katselija"), jotta matriisit ovat vertailukelpoisia ja kokonaiskuva on ymmärrettävä myös järjestelmärajat ylittäen.

5.3 Käyttäjätason koostaminen

Kun järjestelmäkohtaiset matriisit yhdistetään, yksittäisen käyttäjän kokonaisyhteisyydet muodostuvat hänelle myönnettyjen roolien summana kaikissa järjestelmissä, joihin hänellä on pääsy. Tämä koostenäkymä on edellytys kattavalle käyttövaltuuksien hallinnalle.

5.4 Ristikkäisten oikeuksien tunnistaminen (SoD)

Kokonaiskuvasta voidaan tunnistaa tehtävien eriyttämiseen (Segregation of Duties, SoD) liittyviä riskejä, esimerkiksi tilanteita, joissa sama rooli tai henkilö voi sekä luoda että hyväksyä saman prosessin tapahtumia useassa järjestelmässä. Tällaiset havainnot raportoidaan asianomaisille järjestelmien omistajille korjaavia toimenpiteitä varten.

5.5 Raportointi

Koottu kokonaiskuva toimii pohjana säännölliselle käyttövaltuusraportoinnille johdolle, sisäiselle tarkastukselle ja tarvittaessa ulkoisille auditoinneille.

6. Dokumentaation hallinta

Jotta yksittäiset matriisit ovat helposti löydettävissä ja koostettavissa kokonaisuudeksi, dokumentaatiota hallitaan yhtenäisten käytäntöjen mukaisesti:

1. Nimeämiskäytäntö: esim. RBAC_<Järjestelmä>_<vvvv-kk>_v<versio>.pdf.
2. Tallennuspaikka: keskitetty, pääsynhallittu arkisto — ei henkilökohtaisilla työasemilla tai jaetuilla verkkoasemilla ilman pääsynhallintaa.
3. Versiointi: versionumero kasvaa jokaisen katselmoinnin tai muutoksen yhteydessä, ja muutosloki dokumentoidaan matriisin yhteyteen.
4. Pääsynhallinta: matriisit sisältävät tietoturvan kannalta arkaluonteista tietoa, joten niihin pääsy rajataan tarpeen mukaan.

7. Tarkistuslista järjestelmän omistajalle

Ennen matriisin hyväksymistä ja arkistointia järjestelmän omistaja varmistaa, että:

- ☐ Matriisi on ajan tasalla viimeisimmän katselmoinnin mukaisesti.
- ☐ Kaikki roolit ja moduulit on nimetty selkeästi ja yhdenmukaisesti.
- ☐ Jokaiselle solulle on valittu oikeus, lomakkeessa ei ole jäljellä täyttämättömiä "(valitse)"-kenttiä.
- ☐ Määritellyt oikeudet noudattavat vähimpien oikeuksien periaatetta.
- ☐ Matriisi on hyväksytty ja arkistoitu oikeaan, pääsynhallittuun sijaintiin.
- ☐ Seuraava katselmointipäivä on kirjattu kalenteriin ja ilmoitettu tietoturvalle/käyttövaltuushallinnalle.