ØKONOMISTYRELSEN

3. Appendiks
Kontrol af privilegerede rettigheder i IndFak og RejsUd

April 2021

2021

Indhold

1. Kontrol af privilegerede rettigheder i IndFak og RejsUd **4**
1.1 Baggrund 4
1.2 Omfang 4
Er der oprettet brugere med privilegerede rettigheder, der ikke har et godkendt arbejdsbetinget behov? 5
Er der sket en tildeling af prokura til en bruger der har rollen Lokal systemadministrator, der ikke kan begrundes? 6
Har en bruger med rollen **Lokal systemadministrator** tildelt prokura til en anden bruger, der ikke kan begrundes? 7
Har en bruger med rollen **Lokal systemadministrator** oprettet andre brugere med rollen **Lokal systemadministrator**, der ikke kan begrundes? 8
Har en bruger med rollen **Lokal systemadministrator** foretaget en ændring af e-mail eller password på en anden bruger, der ikke kan begrundes? 9

Kontrol af privilegerede rettigheder i IndFak og RejsUd

1. Kontrol af privilegerede rettigheder i IndFak og RejsUd

Denne vejledning beskriver manuelle kontroller af brugere med privilegerede rettigheder, som skal foretages af institutionen selv.

1.1 Baggrund

Det er institutionens ansvar at foretage rettighedskontroller i egen institution, herunder kontrol af egne privilegerede brugere. Kontrollerne skal gennemføres med udgangspunkt i institutionens valg af organisering og samlede risikobillede. Afhængigt af institutionens organisering vil denne vejledning derfor skulle anvendes af systemadministratorer og/eller controllere ude i institutionen.

1.2 Omfang

Systemerne IndFak og RejsUd indeholder brugerroller med særlige privilegier og med udvidet adgang. For at undgå svig og misbrug i systemer, skal tildelingen af disse roller løbende kontrolleres internt, ligesom resultatet af kontrollen efterfølgende skal godkendes ved den ansvarlige personaleleder.

Kontroller der skal foretages i forhold til privilegerede brugere:

1. Er der oprettet brugere med privilegerede rettigheder, der ikke har et godkendt arbejdsbetinget behov?
2. Er der sket en tildeling af prokura, til en bruger, der har rollen Lokal systemadministrator, der ikke kan begrundes?
3. Har en bruger med rollen Lokal systemadministrator tildelt prokura til en anden bruger, der ikke kan begrundes?
4. Har en bruger med rollen Lokal systemadministrator oprettet andre brugere med rollen Lokal systemadministrator, der ikke kan begrundes?
5. Har en bruger med rollen Lokal systemadministrator foretaget en ændring af e-mail eller password på en anden bruger, der ikke kan begrundes?

Er der oprettet brugere med privilegerede rettigheder, der ikke har et godkendt arbejdsbetinget behov?

Der skal dannes et øjebliksbilede af, hvorvidt brugere med privilegerede rettigheder har et godkendt arbejdsmæssigt og/eller funktionsbetinget behov, for netop disse rettigheder for både IndFak og RejsUd.

Roller der skal kontrolleres:

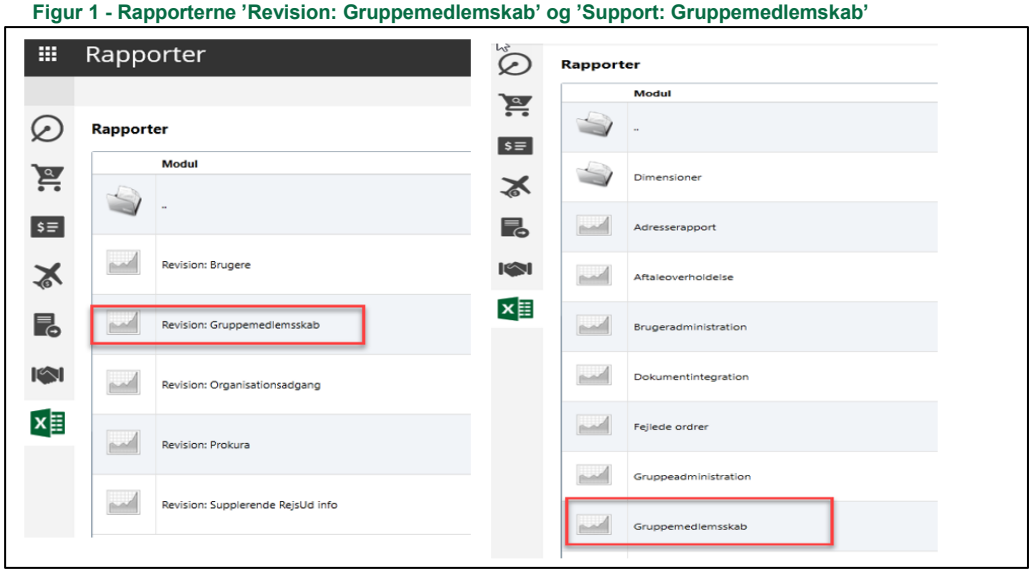
- Rolle IndFak: Lokal systemadministrator
- Rolle IndFak: Disponent
- Rolle RejsUd: Lokal systemadministrator
- Rolle RejsUd: Godkender

Vælg stien: *Administrationsdel\Rapporter\ Revision\Gruppemedlemskab, Periode*
Rapporten REVISION: GRUPPEMEDLEMSKAB viser de roller der er tildelt/slettet for den valgte periode.

Vælg stien: *Administrationsdel\Rapporter\Support\Gruppemedlemskab*. Sæt hak i feltet 'Med underorganisationer'.
Rapporten SUPPORT: GRUPPEMEDLEMSKAB viser et øjebliksbillede af roller.

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.

Figur 1 - Rapporterne 'Revision: Gruppemedlemskab' og 'Support: Gruppemedlemskab'



Handling:

- Resultatet kommenteres, herunder om der er behov for justeringer i brugere med privilegerede rettigheder.
- Rapporten inkl. kommentarer udskrives og underskrives af kontrollant, samt ledelsesgodkendes.

Er der sket en tildeling af prokura til en bruger der har rollen Lokal systemadministrator, der ikke kan begrundes?

En bruger med rollen **Lokal systemadministrator** kan ikke danne transaktioner i IndFak og RejsUd, uden yderligere roller og prokura, og har som udgangspunkt heller ikke brug for dette. Men en bruger med rollen **Lokal systemadministrator** kan godt tildele roller og prokura til en anden bruger med rollen **Lokal system-administrator**. Det er derfor kritisk at undersøge, om dette er sket, eller om en bruger med tildelt prokura skifter rolle til **Lokal systemadministrator** uden til-strækkelig dokumentation herfor.

Roller der skal kontrolleres:

- Rollen IndFak: Lokal systemadministrator
- Rollen RejsUd: Lokal systemadministrator

Til kontrollen skal, ud over resultatet fra rapporterne, REVISION – GRUPPEMED-LEMSKAB og SUPPORT – GRUPPEMEDLEMSKAB, rapporten ÆNDRING AF BELØBS-GRÆNSER anvendes.

Vælg Stien: *Fakturadel\Rapporter\Ændring af beløbsgrænser, Start – Slut periode*
Rapporten ÆNDRING AF BELØBSGRÆNSER viser ændringer af beløbsgrænser, hvem der har foretaget ændringen og hvornår den har fundet sted.

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.

Figur 2 – Rapporten Ændring af beløbsgrænser

Handling:

- Resultatet kommenteres med oplysninger om, hvem der har fået rollen/rol-lerne og prokura. Dokumentationen skal indeholde en ledelsesmæssig beslut-ning for tildelingen.
- Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Har en bruger med rollen **Lokal systemadministrator** tildelt prokura til en anden bruger, der ikke kan begrundes?

Tildelingen af prokura skal ske ved Lokal systemadministrator på samme niveau, som prokuraen skal anvendes. Men en bruger, med lokal administratoradgang, kan tildele roller og prokura til en vilkårlig anden bruger, uden der findes et arbejdsbetinget behov herfor. Derfor er det kritisk at undersøge, om der er sket en tildeling med tiltrækkelig dokumentation for et arbejdsbetinget behov.

Roller der skal kontrolleres:

- Rollen IndFak: Lokal systemadministrator
- Rollen RejsUd: Lokal systemadministrator

Vælg stien: *Fakturadel\Rapporter\Ændring i beløbsgrænser, Start – Slut periode*

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.

Se Figur 2 – Rapporten Ændring af beløbsgrænser

Handling:

- Resultatet kommenteres med oplysning om, hvem der har fået rollen/rollerne og prokura. Dokumentationen skal indeholde en ledelsesmæssig beslutning.
- Rapporten inkl. kommentarer og dokumentation underskrives og udskrives af kontrollant, samt ledelsesgodkendes.

Har en bruger med rollen **Lokal systemadministrator** oprettet andre brugere med rollen **Lokal systemadministrator**, der ikke kan begrundes?
En lokal systemadministrator kan oprette en anden lokal systemadministrator. Det bør undersøges, om der er tilstrækkelig dokumentation herfor.

Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Vælg stien: *IndFak Administrationsdel\Rapporter\Revision\Gruppemedlemsskab, periode*
Rapporten REVISION: GRUPPEMEDLEMSKAB viser de roller der er tildelt/inaktiveret for den valgte periode.

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.

Figur 3 -Rapporten Revision: Gruppemedlemskab

Handling:

- Resultatet kommenteres med oplysning om, hvem der har fået rollen, og hvem der har tildelt rollen. Dokumentationen skal indeholde en ledelsesmæssig beslutning.
- Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Tips:

- Tjek om der er mange forekomster på samme tidspunkt, fx ved at kigge på kolonnen "Sidst ændret" eller "Sidst ændret af".
- Bemærk at flytning af brugere også er en ændring.
- Det er meget tunge regneark. Det kan derfor være nødvendigt at kopiere og indsætte som værdier i et nyt regneark.

Har en bruger med rollen **Lokal systemadministrator** foretaget en ændring af e-mail eller password på en anden bruger, der ikke kan begrundes?

Lokal administrator har adgang til at rette notifikations-e-mail og nulstille password for andre brugere, hvorved det er muligt at logge på som en anden bruger, angive nyt password, og sørge for, at brugerens normale e-mail notifikationer fremsendes til anden bruger end den brugerkonto, der logges på med. Derved bliver det muligt at overtage prokura fra en given bruger på løsningen, uden at brugeren opdager det.

Derfor skal det kontrolleres om dette er sket, og om det i så fald kan begrundes.

Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Vælg stien*: IndFak Administrationsdel\Rapporter\Revision\Brugere, periode*
Rapporten REVISION: BRUGERE viser brugerændringer foretaget på brugere i den valgte periode.

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.

Figur 4 - Rapporten Revision - Brugere

Handling:

- Resultatet kommenteres med begrundelse for ændringen. Dokumentation: mailkorrespondance eller eventuelt sagsnummer.
- Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Tips:

Nogle ændringer kan være legale, som de ændringer der er listet nedenfor, tjek derfor om:

- Ændringen er sket til en "dummy" e-mail konto, fx trash@

- Der evt. er et fejlagtigt "blank" tegn efter den oprindelig email
- Der er tegn på, at den oprindelige e-mail blot var oprettet forkert, fx forkert angivet
- Der er tegn på, at ændringen er sket indenfor institutionens domæne
- Ændringen kan være udført i forbindelse med en ressortomlægning

oes.dk