

# Sådan anvender vi Aula sikkert i Aabenraa Kommune

## Sikkerhedsstrategiske foranstaltninger

Aulas konsekvensanalyse medfører mitigerende foranstaltninger som skal sikre en nedjustering af de identificerede risici til et acceptabelt niveau samt en residualrisiko på lav- henholdsvis middelniveau. Den sikre anvendelse af Aula medfører derudover en præcisering af tjenesternes anvendelsesmulighed samt anvendelsesprioritet.

## Indholdsfortegnelse

|                                                                                        |           |
|----------------------------------------------------------------------------------------|-----------|
| <b>1. Aula-Release.....</b>                                                            | <b>2</b>  |
| <i>Alle brugere skal være fortrolige med indholdet af den nyeste Aula-Release.....</i> | <i>2</i>  |
| <b>2. Kommunikation .....</b>                                                          | <b>3</b>  |
| Anmeldelser .....                                                                      | 3         |
| Sikkerhedshændelser.....                                                               | 3         |
| Alvorlige sikkerhedsbrud .....                                                         | 3         |
| <b>3. Brugernavn og adgangskode .....</b>                                              | <b>4</b>  |
| <b>4. Adgangsstyring.....</b>                                                          | <b>4</b>  |
| <b>5. Aula - tjenesternes anvendelsesmulighed .....</b>                                | <b>6</b>  |
| Overblik / Dashboard.....                                                              | 6         |
| Kalender .....                                                                         | 6         |
| Beskeder .....                                                                         | 6         |
| Opslag .....                                                                           | 7         |
| Dokumenter.....                                                                        | 7         |
| Sikker Fildeling .....                                                                 | 7         |
| Fælles Filer .....                                                                     | 7         |
| Link til OneDrive .....                                                                | 8         |
| Galleri .....                                                                          | 8         |
| <b>Hvad er personoplysninger? .....</b>                                                | <b>9</b>  |
| Almindelige oplysninger (ikke-følsomme personoplysninger) .....                        | 9         |
| Følsomme personoplysninger (særlige kategorier af personoplysninger) .....             | 9         |
| Fortrolige oplysninger.....                                                            | 9         |
| <b>Kontrol af adgangsrettigheder i Aula (spørgeskema) .....</b>                        | <b>11</b> |
| Rettighedstildeling .....                                                              | 11        |
| Vejledning til blankettens spørgsmål.....                                              | 11        |

# 1. Aula-Release

Aula bliver løbende forbedret og opdateret på baggrund af erfaringer og ønsker fra brugerne. Herved udvikler Aula løbende på deres funktionalitet.

## Alle brugere skal være fortrolige med indholdet af den nyeste Aula-Release

På aulainfo.dk kan der dannes et overblik over, hvilken funktionalitet både kommende og allerede gennemførte releases indeholder. Aula offentliggør kommende og gennemførte releases under <https://aulainfo.dk/guide-til-projektledere/funktionalitet-i-aula/status-paa-nye-funktionaliteter/>

For at målrette brugernes fortrolighed med den nye release, fokuseres på relevante funktionaliteter relateret til institutionen. Ikke alle funktionaliteter understøttes af institutionen.

Processen der henfører til en målrettet vidensdeling bør gennemføres af en fagkyndig person (Aula-superbruger, IT-vejleder, Aula administrator).

## 2. Kommunikation

Kommunikationen omhandler håndteringen af interne anmeldelser og kommunikation af sikkerhedsudfordringer til den kommunale administrator.

### Anmeldelser

Skolens Aula-administrator modtager anmeldelser fra brugerne i modulet *Administration* (Administration/Indstillinger/Anmeldelser). Under *Anmeldelser* vises en oversigt over hvilket indhold, der er blevet anmeldt. Samtidig kan der vælges, hvordan håndteringen af det anmeldte indhold skal foregå. *Anmeldelser* viser:

- Det anmeldte indhold
- Hvem har anmeldt indholdet?
- Begrundelse for anmeldelsen
- Link til det anmeldte indhold
- Afsender af det delte indhold

### Sikkerhedshændelser

Sikkerhedsudfordringer i forbindelse med Aula og det anmeldte indhold, som ikke kan løses lokalt på skolen, kommunikeres til Aabenraa Kommunes Aula postkasse henholdsvis gennem telefonopkald. Her modtages spørgsmål og fejlmeldinger. Kan disse ikke løses kommunalt, vil fejlmeldingen blive sendt videre til Aula.

- Postkassen kontaktes under [aula@aabenraaskoler.dk](mailto:aula@aabenraaskoler.dk)
- SkoleIT kontaktes under 2136 5046 (mandag-torsdag kl. 7.00-16.00; fredag kl. 7.00-14.00)
- Stabens rådighedsvagt kontaktes udenfor SkoleIT åbningstider 3063 2544

### Alvorlige sikkerhedsbrud

Sikkerhedsbrud der har betydning for fortroligheden, integriteten eller tilgængeligheden til personoplysninger, meldes til den nærmeste leder. Uanset processen i forhold til eliminering, reducere eller accept af sikkerhedsbruddet, udfyldes en hændelseslog af den nærmeste leder, som sendes til IT-afdelingen. LINK (medarbejderportalen):

<https://medarbejderportalen.aabenraa.dk/hjaelp-til-alle/it-og-digitalisering/informationssikkerhed/haendelseslog/>

### 3. Brugernavn og adgangskode

Man kan som personale logge på Aula på følgende måder:

- Unilogin > Lokalt Login (OS2faktor login)
- Unilogin > MitID
- Fælleskommunal Adgangstyring (kun for brugere på Aabenraa-domænet)
- Kommunal IDP (OS2faktor login)

Brugernavne samt tilhørende adgangskoder må ikke gemmes eller opbevares hverken digitalt eller fysisk.

OS2faktor tilbyder en tjeneste for det pædagogiske personale, som hjælper eleven med at få en ny adgangskode samt at håndtere kravene om øget sikkerhed. Tjenesten tilgås under [kode.aabenraa.dk](https://kode.aabenraa.dk)

Alle brugere skal orienteres omkring sikker opbevaring af brugernavn, adgangskode og 2-faktor enhed som led i den digitale dannelse.

### 4. Adgangsstyring

Adgangsstyringen styrer adgangen til Aula og dens funktionalitet. De lokale administratorer (Aula, TEA) på skolen kan tildele og fjerne roller og rettigheder til enkelte brugere og grupper. Tildelingen af yderlige rettigheder og roller kræver en *eksplicit* grund, hvilken ofte er koblet til en funktion eller opgave på skolen. Tildelingen af rettigheder og roller skal med jævne mellemrum gennemses og, hvis nødvendigt justeres, i det udvidelsen af personkredsen med yderlige rettigheder og roller medfører et højere risiko for eventuelle sikkerhedsbrud.

I forhold til roller og rettigheder i Aula skal der være en øget fokus på følgende (uddrag fra *Administration Roller og rettigheder, Version 1.2*):

- **Bestyrelsesmedlem**  
En elev eller en forælder kan tildeles denne rettighed, som giver de samme muligheder som en kontaktforælder. Derudover kan bestyrelsesmedlemmer tilgå en liste over kontaktforældrenes kontaktoplysninger.
  - **Kontaktforælder:** Giver en bruger af profiltypen "Forælder" mulighed for at tilføje en beskrivelse på sin profil samt en begrænset adgang til sikre filer. Dette indebærer muligheden for at oprette sikre filer og dele disse med institutionens medarbejdere. Bemærk dog, at dokumenterne ikke kan deles med – og derfor ikke vil være synlige for – andre kontaktforældre, ligesom de ikke kan deles med forældre og elever, der ikke har fået tildelt den nævnte rolle. Medarbejdere har ligeledes ikke mulighed for at dele en sikker fil med kontaktforældre.
- **Institutionsadministrator**  
En institutionsadministrator kan håndtere:

- Anmeldelser og slet indhold
  - Supplerende Stamdata og tilladelser
  - Brugerroller
  - Ressourcer på institutionen
  - Planlægning af Komme/Gå
  - Fællespostkasser
  - Fælles Filer
  - Grupper
  - Dashboards
- **Relater sikre filer til alle grupper**  
Giver en medarbejder mulighed for at fremsøge alle institutionens grupper i "omhandler gruppe"-feltet. Det er dermed muligt at oprette sikre filer på alle grupper indenfor institutionen. Rettigheden kan kun tildeles medarbejdere
  - **Se kontaktoplysninger for alle på institutionen**  
Med denne rettighed får medarbejderne mulighed for at se en liste over kontaktoplysninger på brugere i grupper, de ikke selv er en del af.
  - **Se navnebeskyttelse**  
Giver brugere med profiltypen 'medarbejdere' mulighed for at se, om en bruger er navnebeskyttet eller ej. Dette sker gennem rettigheden 'Se navnebeskyttelse'. Alle medarbejdere med rollerne 'Leder', 'Ledelse', 'Lærer', 'Pædagog', 'Konsulent' bliver automatisk tildelt denne rettighed.
  - **Se stamkortoplysninger for alle på institutionen**  
Giver medarbejdere mulighed for at se en liste over alle stamkortoplysninger for alle børn og forældre indenfor institutionen. Stamkortoplysninger omfatter tilladelser, supplerede stamdata og samtykker.
  - **Sikker fildeling, fuld institutionel adgang**  
Giver medarbejdere mulighed for at se og redigere alle sikre filer på institutionen, uanset om de er delt med brugeren eller ej. Rettigheden skal tildeles af en administrator og kan kun tildeles til medarbejdere på en skole eller et dagtilbud, dvs. ikke på den kommunale institution.
  - **SkoleIntra arkiv administrator**  
Giver en medarbejder mulighed for at tilgå al den data, der er overført fra Skoleintra til Aula inklusiv alt migreret/arkiveret data på hele institutionen. Rettigheden giver vedkommende også adgang til medarbejdernes arkiverede beskeder. Det er derfor vigtigt, at skolen har instrukser eller klare retningslinjer for, hvem der skal have denne rettighed, og evt. om dette er en tidsbegrænset adgang.

Der kan læses mere om roller og rettigheder under *Administration Roller og rettigheder, Version 1.2* <https://aulainfo.dk/wp-content/uploads/Roller-og-rettigheder-i-Aula.pdf>

## 5. Aula - *tjenesternes anvendelsesmulighed*

### Overblik / Dashboard

Overblik viser de aktuelle opslag. Derudover indgår overbliksiden i Aulas dashboard, som kan tilpasses den enkelte brugergruppe. Dashboardet skal gerne indeholde de mest relevante informationer tilpasset til den enkelte brugergruppe (se administration/opsætning/Dashboards). Fx det pædagogiske personale:

- Linksamling (EasyIQ)
- Office365 Dashboard
- Dagens fravær
- Dagens skema

### Kalender

Alle aktiviteter og begivenheder bliver samlet i kalenderen. Det samlede overblik omfatter

- Skema (lærernes skema / klasseskema / faglokale skema)
- Vikarskema
- Begivenheder (Skole-hjem-samtale / møder / MUS-samtale)
- Skolens kalender

Kalenderen i Aula kan synkroniseres (en-vej-synkronisering) med eksterne kalenderkonti. For at opsætte kalendersynkroniseringen, tilgås kalendermodulet og efterfølgende *kalendersynkronisering* i værktøjslinjen.

Skemabrikker og vikarnoter bruges til at oprette noter til vikaren henholdsvis noter til klassen. Notefunktionen til klassen kan bruges som en lektiebog.

Funktionen *ferieanmodninger* giver et overblik over hvor mange og hvilke børn der kommer henholdsvis ikke kommer i institutionen i forbindelse med den specifikke ferieanmodning.

### Beskeder

Aula beskedsystem bruges til at sende en besked til én eller få personer med en forventning om et svar.

- Indeholder beskeden følsomme personoplysninger, skal beskeden mærkes med *marker som følsom* - både ved beskeder til forældre og beskeder ansatte imellem.
- Vælg Opret en besked enkeltvist til hver modtager, hvis modtagerne ikke skal kende de øvrige modtagere eller have mulighed for at kommunikere i en fælles beskedtråd.
- Beskedsystemet kan anvendes som kontaktbog f.eks. ved sygdom, hvor forældrene kan sende en besked direkte til klasselæreren. Rummer beskeden følsomme personoplysninger, kan både forældre og klasselærer markere beskeden som følsom.
- En *Fællespostkasse* kan også bruges til kontaktbog.

## Opslag

I modsætning til beskedsystemet har opslagsfunktionen en informerende karakter, hvor der ikke forventes et svar.

- Opslag skal målrettes til en eller flere grupper.
- Opslag kan markeres som *vigtig*, hvilket giver modtagerne mulighed for at sortere i opslagene på deres overblik.
- Opslag skal være aktuel og relevant.
- Der er mulighed for at kunne kommentere på indholdet af et opslag.

## Dokumenter

Dokumenter indeholder genveje til forskellige *Filer og dokumenter*. Herunder *Sikker Fildeling*, *Fælles Filer* og *Link til fil i OneDrive*.

### Sikker Fildeling

Sikker Fildeling kræver to-faktor-login og giver muligheden for at gemme og dele følsomme personoplysninger sikkert. Data skal tilknyttes et barn.

- Sikker Fildeling bruges til at samle vigtige informationer omkring barnet.
- Relevant personale har læse- henholdsvis skriveadgang til Sikker Fildeling.
- Sikker Fildeling kan bruges som klasselog.
- Der kan filtreres på det enkelte barn.

Se vejledningen for Sikker Fildeling på <https://pucaabenraa.aula.dk/aula/vejledninger>

**Sikker Fildeling må IKKE bruges til journalisering. Alt journalisering skal foregå i Acadre.**

### Fælles Filer

Fælles Filer samler institutionens fælles filer. Som bruger har man kun en læseadgang til *Fælles Filer*. Det vil sige, at man ikke kan ændre i filerne eller tilføje filer til mappen. *Fælles Filer* kan være:

- Virksomhedsplaner
- Strategier
- Mobbepolitik
- Referater fra bestyrelsesmøder

Den kommunale administrator, institutionsadministratoren og medarbejder, der har fået tildelt rettigheder hertil, kan uploade PDF-dokumenter i *Fælles Filer*.

**HUSK:** *Datapolitik i Aabenraa Kommune* skal gemmes i Fælles Filer hos alle institutioner:

[https://aabenraa.sharepoint.com/:b:/s/PUCAabenraa/EUny3duOZodDjwkX\\_aNxwMYBC8V6pcrcVv9ba2RnXGJhTw?e=qchLmi](https://aabenraa.sharepoint.com/:b:/s/PUCAabenraa/EUny3duOZodDjwkX_aNxwMYBC8V6pcrcVv9ba2RnXGJhTw?e=qchLmi)

## Link til OneDrive

Aula har ikke et dokumentlager, hvor den enkelte bruger kan gemme og dele filer og dokumenter. Dokumenter, der ikke indeholder personfølsomme oplysninger, gemmes i Microsoft OneDrive. OneDrive tilgås i dokumentmodulet *Link til OneDrive*.

Læs mere om OneDrive samt de enkelte Office 365 applikationer på <https://pucaabenraa.aula.dk/office-365/vejledninger>

***Office 365 er ikke godkendt til at gemme følsomme personoplysninger.***

## Galleri

I galleriet kan der ses og deles billede-, video- og lydfiler. Galleriet differentierer *ikke længere* mellem *Portrætbilleder* og *Situationsbilleder*. Visningen af billeder er ikke længere afhængig af, om der gives samtykke.

Baggrunden for ændringerne er, at Datatilsynet har vurderet, at det er væsentligt for institutioners virke at kunne gemme og bruge fotos, og at man derfor ikke behøver at bede om samtykke.

Datatilsynet har, efter drøftelse i Datarådet, besluttet at ændre praksis i forhold til at skelne mellem portrætbilleder og situationsbilleder. Fremadrettet skal offentliggørelsen af billeder bero på en helhedsvurdering af billedet samt dets formål med offentliggørelsen. Vurderingen, på hvilket behandlingsgrundlag et billede af en identificerbar person kan offentliggøres, gennemføres af den dataansvarlige.

Overstående proces gælder kun i forbindelse med brugen af Galleri i Aula. Brugen af billede-, video- og lydfiler på skolens hjemmeside og andre portaler, kræver samtykke.

# Hvad er personoplysninger?

Personoplysninger er informationer, der kan henføre til en bestemt person, ligeledes om identifikationen kræver en kombination med andre oplysninger. Behandling af personoplysninger kræver altid samtykke.

## Almindelige oplysninger (ikke-følsomme personoplysninger)

Denne kategori omfatter alle oplysninger, der ikke er klassificeret som følsomme personoplysninger.

Eksempel:

- Navn og adresse
- Mail
- Telefonnummer
- Betalingsoplysninger

## Følsomme personoplysninger (særlige kategorier af personoplysninger)

Disse oplysninger er udtrykkelig afgrænset i databeskyttelsesforordningen. Adgangen til behandling af disse oplysninger er snævrere end ved almindelige oplysninger. Med mindre, man har udtrykkeligt samtykke til at behandle følsomme personoplysninger til et specifikt formål, er det ikke tilladt at behandle disse oplysninger.

Det er oplysninger om:

- Race eller etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering

## Fortrolige oplysninger

Fortrolige oplysninger defineres gennem straffelovens §152 sammenhold med forvaltningslovens §27. Sådanne oplysninger kan være underlagt særlige beskyttelsesbehov. Samtidig vil de ofte være underlagt særregulering i anden lovgivning. Følsomme personoplysninger er altid også fortrolige oplysninger, men ikke nødvendig omvendt.

En oplysning kan anses for at være fortrolig, hvis den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab jf. straffelovens §152 sammenhold med forvaltningslovens §27.

Fortrolige oplysninger kan være:

- Indtægts- og formueforhold
- Arbejds-, uddannelses- og ansættelsesmæssige forhold
- Interne familieforhold
- Selvmordsforsøg og ulykkestilfælde
- CPR-nummer

Oplysninger, der ikke kan nægtes udleveret og som dermed ikke er deklareret fortroligt, vil være oplysninger af rent objektiv karakter (fx i forhold til udstedelse af pas, kørekort osv.)

Der kan læses mere om personoplysninger på:

- <https://www.datatilsynet.dk/databeskyttelse/hvad-er-personoplysninger>
- <https://gdpr.dk/persondataforordningen/hvad-er-personoplysninger/>
- <https://medarbejderportalen.aabenraa.dk/hjaelp-til-alle/it-og-digitalisering/informationssikkerhed/information-omkring-databeskyttelsesreglerne/>

# Kontrol af adgangsrettigheder i Aula (spørgeskema)

Inden for en tidsperiode på 6 måneder skal blanketten *Kontrol af adgangsrettigheder i Aula - skolerne* udfyldes. Herved gennemføres en kontrol af tildelte rettigheder i Aula. Blanketten sendes ud 2x årligt gennem forvaltningsinstitutionen Skole og Undervisning.

Efterfølgende vejledning tager udgangspunkt i blankettens spørgsmål.

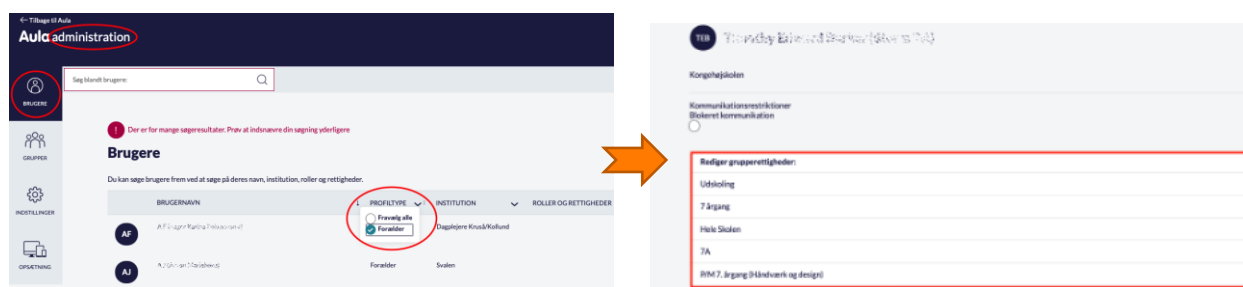
## Rettighedstildeling

| Rolle / bruger                                                          | Ansvarlig for tildeling af rettigheder                                        |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Kommuneadministrator                                                    | Skolechef<br><i>i sammenspil med kommuneadministratorene (SkoleIT og PUC)</i> |
| Administrationsadministrator                                            | Skoleleder<br><i>i sammenspil med institutionsadministrator</i>               |
| Almene brugere<br>(medarbejder, forældre, elever, eksterne fagpersoner) | Skoleleder<br><i>i sammenspil med institutionsadministrator</i>               |

## Vejledning til blankettens spørgsmål

1. Har I gennemført en stikprøve med 10 forældre og 10 elever for at kontrollere, at de ikke har rettigheder, som giver adgang til flere grupper end højest nødvendigt?

For at kunne gennemføre stikprøven anbefales at tilgå administrationsmodulet i Aula, hvilket kræver en to-faktor-login. Efterfølgende vælges modulet *BRUGERE*. For at kunne kontrollere forældrene, vælges profiltypen *Forælder*. Ud fra listen fremgår alle forældre som er tilknyttet til institutionen. Kontrollér rettighederne i forhold til gruppetildelingen.

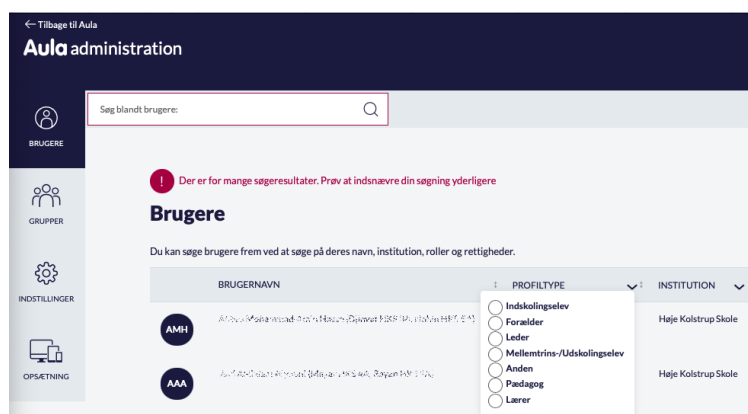


Gentag overstående proces i forhold til indskolings elever og mellemtrins-/udskolings elever.

2. Har I kontrolleret alle medarbejdere i Aula, for at sikre, at der ikke er forhenværende medarbejdere? \*
3. Har I kontrolleret alle eksterne personer, for at sikre, at de ikke har uberettigede adgange? \*
4. Har I kontrolleret, at forhenværende medarbejdere fra eksterne institutioner ikke har adgang til skolens Aula? \*

\*) Overstående 3 spørgsmål kan kontrolleres under samme proces.

For at kunne gennemføre kontrollen anbefales at tilgå administrationsmodul i Aula, hvilket kræver en to-faktor-login. Efterfølgende vælges modulet *BRUGERE*. Under profiltipe vælges i første omgang *Leder*. Kontrollér at der ikke er forhenværende brugere.



Gentag overstående proces for profiltypen *Anden*, *Pædagog* og *Lærer*.

I forhold til roller og rettigheder skal der kontrolleres for eksternes rettigheder (fx *Sikker fildeling*, *fuld institutionel adgang*, *se kontaktoplysninger for alle på institutionen* eller *se navnebeskyttelse*). Som udgangspunkt skal der tildeles færrest mulige rettigheder.

## 5. Har I kontrolleret, at eksterne medarbejdere ikke har adgang til *Sikker Fildeling*?

For at kunne gennemføre kontrollen anbefales at tilgå administrationsmodulet i Aula, hvilket kræver en to-faktor-login. Efterfølgende tilgås ekstern medarbejders profil under *Brugere*. Der kontrolleres for adgang / tilknytning til grupper. Den eksterne medarbejder må **ikke** have adgang til grupper der indeholder elever. Dette kontrolleres ved at klikke på brugeren og tjekke at der er *ingen grupper tilgængelige*. I tilfælde af tilgængelige grupper, skal der sikkerstilles, at der ikke er tilkoblet elever til samme gruppe.



## 6. Har I kontrolleret, at der ikke er forhenværende institutionsadministratorer, der fortsat har administrator-rettigheder?

For at kunne gennemføre kontrollen anbefales at tilgå administrationsmodulet i Aula, hvilket kræver en to-faktor-login. Efterfølgende vælges modulet *BRUGERE*. Under *ROLLER OG RETTIGHEDER* vælges *Institutionsadministrator*. Kontroller at der ikke er forhenværende brugere med rollen / rettigheden *Institutionsadministrator*.



Stand: 17.08.2022