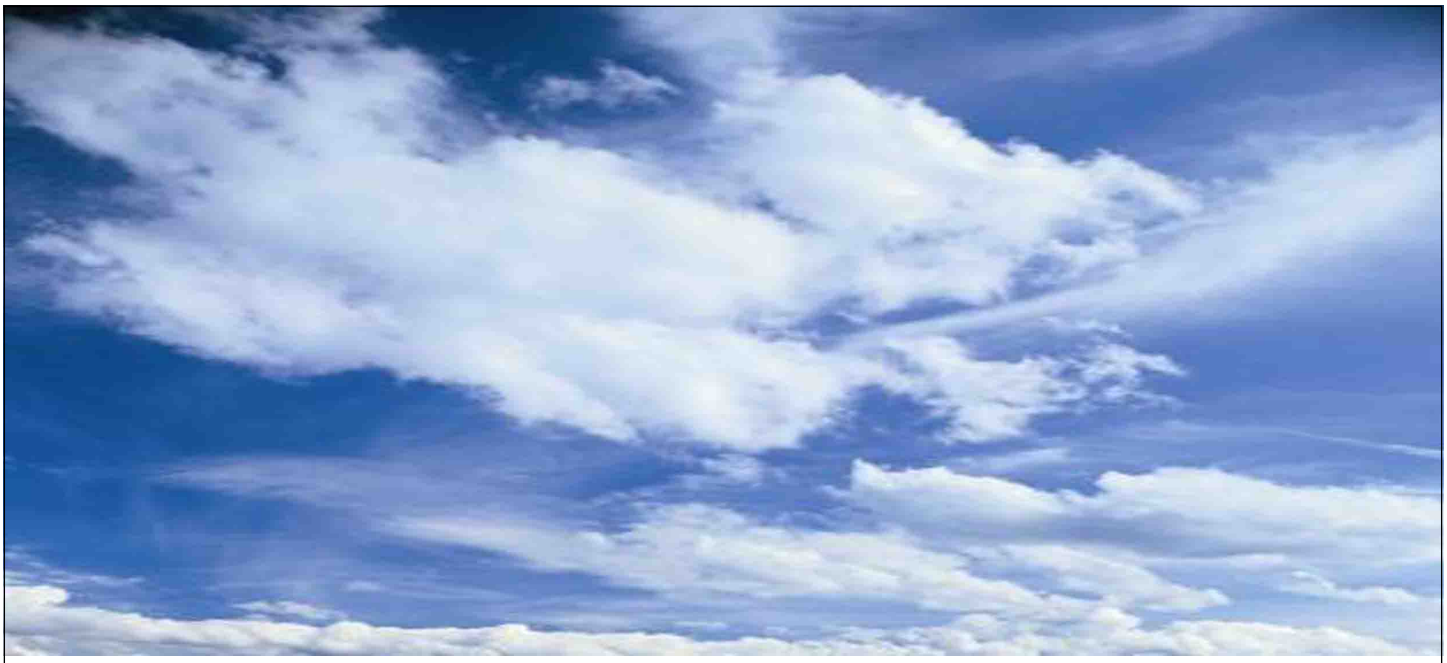


Aabenraa Kommune

Acadre Sikkerhedsindretning for Aabenraa Kommune

Indholdsfortegnelse

Acadres organisationsstruktur

Acadre anvender en organisationsstruktur "Acadrestruktur", hvori sager og dokumenter placeres. Brugerne placeres også i denne struktur, som dermed danner grundlag for indretning af sikkerheden i Acadre.

Rettigheder til sager og dokumenter har direkte sammenhæng til kommunens organisering. Strukturen skal derfor afspejle kommunens organisationsplan.

Efter kommunesammenlægningen blev data fra de 5 gamle kommuner videreført i Acadre, hvorfor de 5 gamle kommuner også er at finde i Acadrestrukturen. Udover Aabenraa Kommunes organisation og de 5 gamle kommuner, er Acadre med tiden blevet udvidet til andre områder, som ligger udenfor den kommunale anvendelse, og til delvist kommunalt styrede selskaber.
Derudover indeholder strukturen også nedlagte kommunale områder, som f.eks. sager, der er overgået til Udbetaling Danmark, Arwos eller Region Sydjylland. Også nedlagte kommunale institutioner er indeholdt i strukturen udenfor Aabenraa Kommune. Disse områder har den almindelige medarbejder under Aabenraa Kommune grundlæggende ingen adgang til, men kan efter en godkendelse fra lederen/direktøren gives adgang hertil.

Alle områder ligger i hver sin gren af Acadrestrukturen, hvor øverste niveau er "Acadre". På denne måde kan man styre adgangen til de forskellige sager. Se bilag 1 - Acadre organisationsstruktur - 01-2017.

Sikkerhed på konverterede data

Beskyttelse af data i de 5 gamle kommuner var opbygget efter de tekniske muligheder, tilgængelige i kommunernes forskellige ESDH-systemer. Ved konverteringen har det ikke været muligt at videreføre denne sikkerhed i alle detaljer. De konverterede data er derfor ikke indrettet med samme detaljeringsgrad, som den ovenfor beskrevne sikkerhed under Aabenraa Kommune.
Adgangskoden "Borgersag" er således generelt anvendt på alle personsager fra de gamle kommuner, også på sager, der vil kunne klassificeres efter kategori 1 – Høj.
I sager fra "Gl. Aabenraa" er adgangskoden "Børnesag" dog anvendt på et mindre antal sager fra den tidligere "Aabenraa-PPR-afdeling".

Indretning af sikkerheden

Sikkerhedsindberetning til IT-afdelingen

Håndtering af Acadres sikkerhed sker i et administrationsprogram, som kun administratorer i IT-afdelingen har adgang til.
Der skal altid foretages en sikkerhedsindberetning til IT-afdelingen ved personales ansættelse, ophør, rokering samt enhver ændring i medarbejdernes arbejdsopgaver, der nødvendiggør en ændret adgang til informationer i Acadre.
Indberetningen foretages i et indberetningsskema, der er udarbejdet og vedligeholdes af IT-afdelingen. Alle indberetninger skal sendes elektronisk til IT-afdelingen via helpdesksystemet.
Indberetningsskemaet anvendes også ved Acadrebrugeres ophør.
Vedrørende brugere, der fratræder, er der udarbejdet en procedure for håndtering af sager og dokumenter. Se bilag 2.

Afslutning af sager og låsning af dokumenter

Uanset hvilken adgangssikkerhed der tilknyttes en sag eller et dokument, er det et overordnet princip i anvendelse af ESDH-systemer, at afsluttede data skal låses.
Den medarbejder, der er ansvarlig for en given sag eller et dokument, skal sørge for at markere sagen som afsluttet ved endt sagsbehandling og sørge for, at dokumenter låses, når de er afsluttede eller ligger til grund for en beslutning.
Principperne om afslutning og låsning er implementeret i Acadre på følgende måde:

Afslutning af sager

Sager, der er færdigbehandlede, skal markeres som afsluttede i Acadre.
Sagsstatus sættes til: A = Afsluttet.
Markeringen er synlig for kolleger, der kan se at en given sag er afsluttet, og har betydning for den senere aflevering til statens arkiver.
Jfr. nedenstående beskrivelse af "Roller", vil alle medarbejdere med "Aktiv adgang til Acadre" (skriveadgang) kunne ændre sagsstatus, med undtagelse af "Afsluttede sager".
Acadresystemet begrænser muligheden for at gøre "Afsluttede sager" aktive igen. Det er således kun brugere med administratorrettigheder til Acadre, der kan foretage denne handling.
Ændringer i en sags status registreres i sikkerhedsloggen.

Instruks for genåbning af sager i Acadre

Der skal oprettes en opgave i helpdesksystemet for at kunne få genåbnet en sag. Opgaven kan oprettes af brugeren eller superbrugeren.
Kun administratorer kan genåbne sager i hele organisationen. Administratorer består af ESDH-teamet i IT-afdelingen.
Der er lavet enkelte undtagelser fra denne regel, hvor rettigheden er tildelt få udvalgte superbrugere. Se bilag 3 - Undtagelser fra Sikkerhedsindretningen.

Instruks for sletning af sager i Acadres papirkurv

Kun administratorer må slette sager fra Acadres papirkurv, hvilket gælder for hele organisationen. Administratorer består af ESDH-teamet i IT-afdelingen.

Låsning af dokumenter

Dokumenter skal låses, når de er afsluttede eller ligger til grund for en beslutning.
Adgangen til at oplåse dokumenter er begrænset i Acadre, så det kun er Administratorer og Superbrugere, der har denne mulighed.
Låste dokumenter bør kun undtagelsesvis låses op, og som udgangspunkt kun på foranledning af den, der har udfærdiget dokumentet.
Låsning og oplåsning af dokumenter registreres i Acadres sikkerhedslog.
Indskannede dokumenter låses automatisk i skanningsprocessen.
Ændringer i et dokuments status registreres i sikkerhedsloggen.

Roller og adgangskoder

Brugernes adgang til data i Acadre bygger på to sikkerhedselementer; "Roller" og "Adgangskoder", beskrevet herunder. Det er summen af brugerens roller og adgangskoder, kombineret med disses placering i organisationen, der udgør brugerens samlede adgang til sager og dokumenter i ESDH-systemet.

Roller

En "Rolle" er et udtryk for hvilke handlinger man har lov til at udføre i Acadre. En bruger tildeles en rolle, der samtidigt knyttes til en "Administrativ enhed" i Acadrestrukturen.
Alle brugere tildeles mindst én rolle som enten er "Sagsbehandlerrollen" eller "Læserrollen".
En bruger kan tildeles flere roller: Én "primær rolle" suppleret med én eller flere "sekundærroller".

Primær rolle

Brugerens "Primær rolle", knyttes til den "Administrative enhed" i Acadrestrukturen, hvor brugeren er ansat.
Den primære rolle placerer brugeren i Acadrestrukturen.

Sekundære roller

Brugeren kan have én eller flere sekundære roller.
En sekundær rolle kan kun udvide brugerens muligheder i Acadre, ikke begrænse dem.

Acadre indeholder følgende roller:

(Rollerne er beskrevet detaljeret i bilag 4)

Sagsbehandler

Beskrivelse:
"Sagsbehandler" er den traditionelle rolle i Acadre.
Som "Sagsbehandler" må man udføre alle de almindelige handlinger i Acadre: Søge – Læse – Oprette – Ændre - Slette.
Anvendelse:
Giver ret til at arbejde med alle sager og dokumenter i Acadre, der ikke er beskyttet af en "Adgangskode". Se afsnittet "Adgangskoder" om beskyttelse af særlige sagsområder. Rollen har virkning i hele Acadrestrukturen, uanset hvilket niveau den tilknyttes.
Tildeling:
Tildeles som primær rolle til alle brugere, der skal arbejde aktivt i Acadre, og tilknyttes den administrative enhed, som medarbejderen er ansat i.

Læser

Beskrivelse:
"Læser" har kun ret til at se sager og dokumenter, og kan dermed ikke oprette, ændre eller slette data.
Anvendelse:
Rollen giver umiddelbart ret til at se alle ubeskyttede sager og dokumenter. Rollen har virkning i hele Acadrestrukturen, uanset hvilket niveau den tilknyttes.
Tildeling:
Tildeles til personer, der kun skal kunne søge og læse i Acadre, f.eks. til revisionen, eller til brugere, der skal kunne se sager fra de gamle kommuner.

Dagsordensamler

Beskrivelse:
"Dagsordensamler" giver mulighed for at arbejde med udvalg og dagsordener.
Anvendelse:
Rollen giver adgang til at arbejde med udvalg og dagsordener i "den administrative enhed som rollen tilknyttes" i Acadrestrukturen. Rollen har kun virkning for medarbejderen på denne ene afdeling og arves hverken op eller ned i Acadrestrukturen.
Tildeling:
Tildeles dagsordensamlere og tilknyttes den eller de administrative enheder hvor medarbejderens aktuelle udvalg er indplaceret. Tildeles som sekundær rolle.

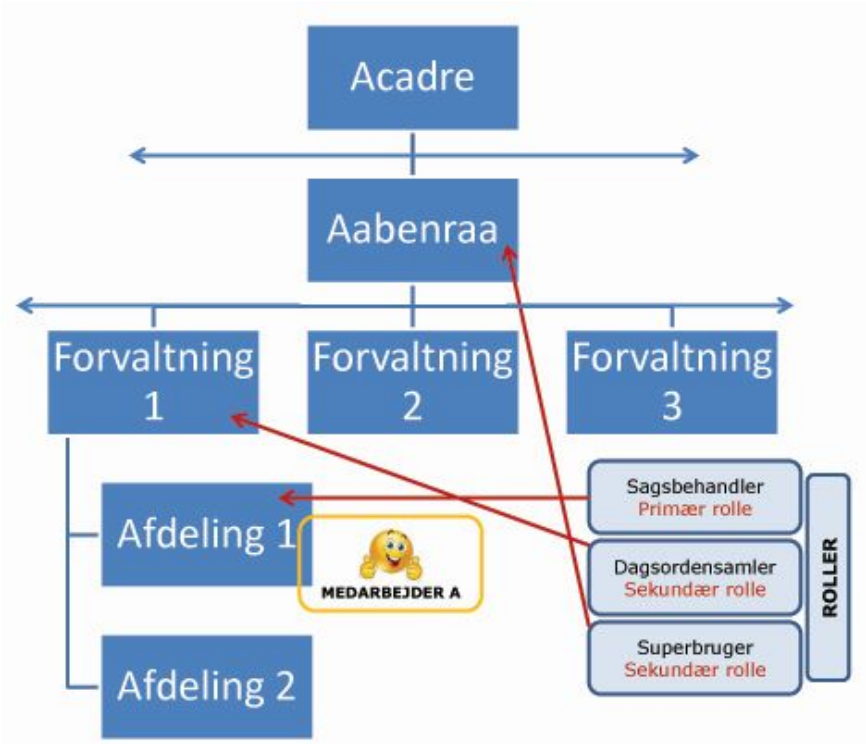
Superbruger

Beskrivelse:
Superbrugerrollen svarer til "Sagsbehandlerrollen", suppleret med adgangen til at oplåse "låste dokumenter".

Anvendelse:
Superbrugere kan oplåse dokumenter i hele Aabenraa Kommune
Tildeling:
Tildeles som sekundær rolle og tilknyttes Aabenraa Kommune
Den Digitale Styregruppe godkender efter indstilling fra afdelingsledere, hvilke personer, der kan udpeges som Acadre superbrugere og dermed tildeles adgangskoden "Superbruger".

Administrator
Beskrivelse:
"Administrator" giver mulighed for at arbejde med den grundlæggende indretning af brugeradgange og sikkerhed i hele Acadresystemet.
Anvendelse:
Tildeles kun sikkerhedsadministratorer
Tildeling:
Tildeles som sekundær rolle.

Eksempel på anvendelsen af primær og sekundære roller



"A" er ansat i "Afdeling 1" i "Forvaltning 1" og er derfor tildelt primærrollen "Sagsbehandler" i "Afdeling 1". Primærrollen placerer "A" i "Afdeling 1".
"A" er også superbruger, og er derfor tildelt sekundærrollen "Superbruger" tilknyttet på niveau "Aabenraa".
"A" er endvidere dagsordensamler, og er derfor tildelt sekundærrollen "Dagsordensamler" tilknyttet den organisatoriske enhed, hvor udvalget, som "A" er dagsordenfører for, er placeret. I dette tilfælde i den administrative enhed "Forvaltning 1".

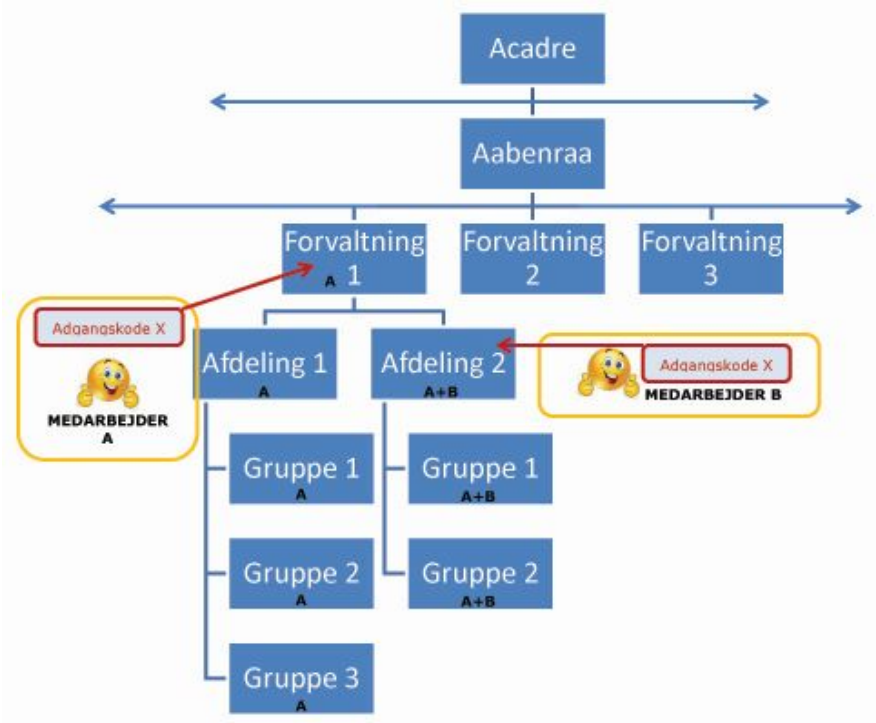
Adgangskoders anvendelse
I Acadre kan sager, dokumenter eller hele sagsområder påføres en særlig beskyttelse. Denne beskyttelse benævnes "Adgangskoder". Fra 1. januar 2007 var systemet indrettet således, at det var muligt at dele sager i hele organisationen, ved at der ikke blev påsat en adgangskode på disse sager eller dokumenter. Det har dog vist sig, at det medfører sikkerhedsmæssige udfordringer, hvorfor det er blevet besluttet, at alle sager og dokumenter SKAL være påført en adgangskode. Systemet kontrollerer automatisk, at det sker.
Adgangskoder tildeles (autoriseres) efter de nedenstående principper og regler (standardmodel) af IT-administrationen, efter anmodning fra afdelingslederen eller delegeret gruppe/institutionsleder. Rekvirenter, der er godkendt af ledere kan udføre det praktiske arbejde med udfyldelse af sikkerhedsindberetninger der indsendes via Helpdesksystemet.

Ved ønske om tildeling af adgangskoder, der rækker ud over de nedenstående regler og principper, skal anmodningen godkendes af afdelingsledere, som har ansvar for (ejer) de beskyttede data, der ønskes adgang til.
Er en bruger tildelt en adgangskode, kan brugeren påføre og ændre adgangskoden fra sager og dokumenter. Brugeren har samtidig adgang til sager og dokumenter påført den aktuelle adgangskode.
Uden at være tildelt den aktuelle adgangskode, kan hverken sagen eller dens dokumenter ses eller fremsøges af brugeren.

Nedarvningsprincippet

En brugers adgangskode knyttes altid til en "Administrativ enhed" i Acadrestrukturen. Adgangskoden virker dermed for brugeren i den administrative enhed som koden er knyttet til og alle underliggende afdelinger i Acadrestrukturen.

Udsnit af Acadrestrukturen med illustration af nedarvningsprincippet:



Medarbejderne "A" og "B" er begge tildelt "Adgangskode X".

"A" er tildelt "Adgangskode X", tilknyttet "Forvaltning 1", og "A" kan dermed tilgå alle sager, der er beskyttet med "Adgangskode X" i hele "Forvaltning 1" og underliggende afdelinger.
"A" vil ikke kunne tilgå sager beskyttet med "Adgangskode X" i andre dele af organisationen.
"B" er tildelt "Adgangskode X" tilknyttet "Forvaltning 1's" "Afdeling 2" og kan kun tilgå sager, der er beskyttet med "Adgangskode X" i "Afdeling 2" og underliggende enheder.
"B" vil ikke kunne tilgå sager beskyttet med "Adgangskode X" i andre dele af organisationen.

Klassifikation af data

ESDH-systemet skal bidrage til åbenhed og gennemsigtighed i sagsbehandlingen samt bidrage til at øge overblikket for den enkelte medarbejder. Derfor er det et mål, at ESDH-systemet indrettes som et åbent system, med så få begrænsninger for adgang til data som muligt.
Det er imidlertid nødvendigt, at data til enhver tid vurderes, sikkerhedsklassificeres og påføres den lovgivne og nødvendige databeskyttelse.
Adgangskoderne i Acadre skal anvendes til at håndhæve sikkerhedsklassifikationerne, idet den enkelte medarbejder ved modtagelse eller produktion af data, skal vurdere og beskytte data efter et af følgende 4 klassifikationsniveauer:

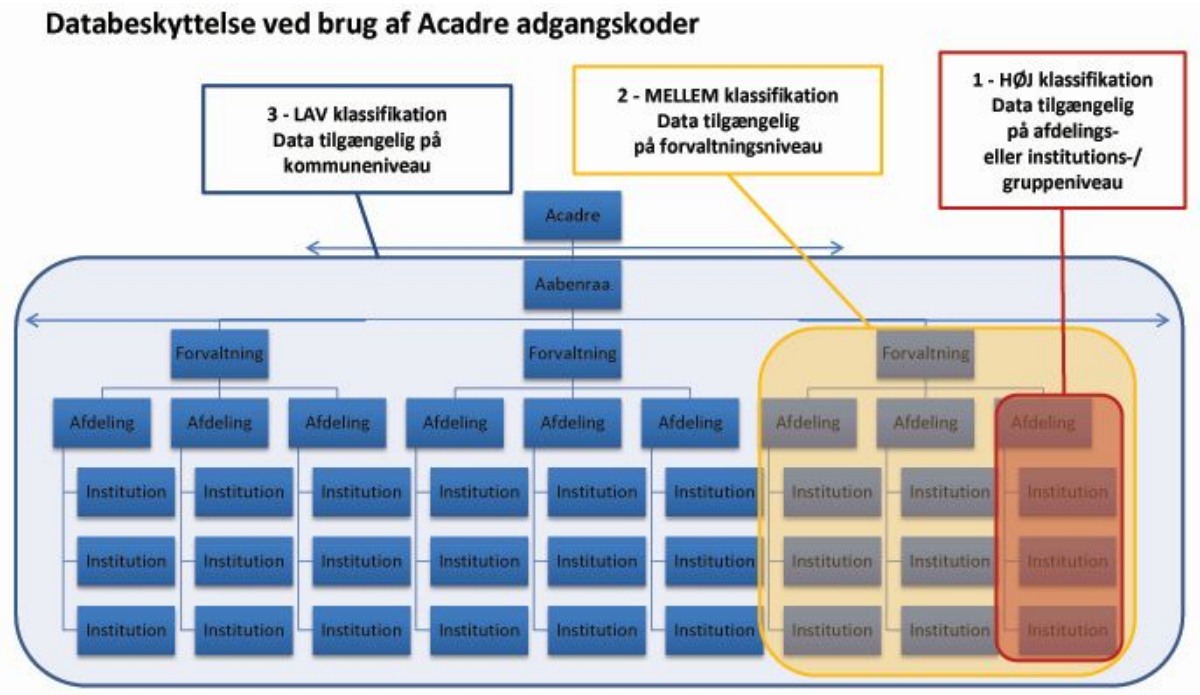
1. Data, der lovgivningsmæssigt skal behandles strengt fortroligt som f.eks. sager jfr. persondatalovens §§ 7 og 8 (herunder børnesager) eller sager underlagt licitationsregler.
   Klassifikation: HØJ
   Data er kun tilgængelig for brugerne på afdelings-, gruppe-, eller for afgrænsede medarbejdergrupper på forvaltningsniveau.

2. Data, der lovgivningsmæssigt skal behandles med en vis fortrolighed som f.eks. sager jfr. persondatalovens § 6 eller administrative sager hvor informationerne kan betegnes som følsomme.
   Klassifikation: MELLEM
   Data er tilgængelig for brugerne på forvaltningsniveau

3. Data i administrative sager hvortil kun administrative medarbejdere bør have umiddelbar adgang.
   Klassifikation: LAV
   Data er tilgængelige for centraladministrationen eller lokalt for institutioner

4. Data i sager hvortil institutioner og eksterne samarbejdsparter (konsulenter m.v. der gives brugeradgang i Acadre) må have umiddelbar adgang.
   Klassifikation: INGEN
   Alle sager i Acadre, der ikke beskyttes af en "Adgangskode" vil som minimum være læsbare for alle brugere af systemet.

Illustration af Acadres adgangskoder, anvendt til sikkerhedsklassifikationerne 1-HØJ, 2-MELLEM og 3-LAV



Adgangskoder i Acadre

Dataklassifikation 1 - Høj

Særlig Borgersag

Dataklassifikation HØJ

Anvendelse

Anvendes på sager og dokumenter, der skal behandles strengt fortroligt. Sager der indeholder oplysninger af privat karakter, jfr. persondatalovens §§ 7 og 8 eller tilsvarende lovgivning; følsomme oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, strafbare forhold, væsentlige sociale problemer og andre rent private forhold.

Tildeling

Tildeles afgrænsede medarbejdergrupper, der arbejder med disse sagstyper i forvaltningerne.
Medarbejdere i den øvrige del af organisationen tildeles som udgangspunkt ikke adgangskoden.

Tilknytning

For medarbejdere i centraladministrationen i de nævnte forvaltninger tilknyttes adgangskoden på forvaltningsniveau.
For medarbejdere uden for centraladministrationen (institutioner under de nævnte forvaltninger) tilknyttes adgangskoden den institution hvor medarbejderen organisatorisk er placeret.

Børnesag

Dataklassifikation HØJ

Anvendelse

Anvendes på sager der skal behandles strengt fortroligt. Sager der indeholder oplysninger af privat karakter, jfr. persondatalovens §§ 7 og 8 eller tilsvarende lovgivning, hvor børn er sagens hovedpersoner, f.eks. ved tvangsfjernelses-, incest-, pædofilisager og sager vedrørende pædagogisk psykologisk rådgivning.
Adgangskoden skal betragtes som en skærpet beskyttelse i relation til adgangskoden "Særlig Borgersag".

Tildeling

Tildeles medarbejdere, der arbejder med de pågældende sagstyper.

Tilknytning

Adgangskoden tilknyttes som udgangspunkt den administrative enhed i Acadrestrukturen, hvor medarbejderen organisatorisk er placeret (hvor primærrollen er tilknyttet).

Personalesag

Dataklassifikation HØJ

Anvendelse

Adgangskoden anvendes på alle personalesager.

Tildeling

Tildeles direktionen, og medarbejdere, der arbejder med personalesager.
Adgangskoden tildeles også chefer og ledere, som har et personaleansvar.
Automatik: Når en medarbejder er tildelt adgangskoden "Personalesag" foreslås denne automatisk af systemet, sat på sager, der oprettes med sagstypen "Personalesag". Se afsnittet "Oprettelse af sager" om "Sagstyper".

Tilknytning

For medarbejdere i HR-afdelingen samt for direktionen tilknyttes koden på niveau "Aabenraa Kommune" og "Gamle Kommuner".
For chefer og ledere med personaleansvar tilknyttes adgangskoden den administrative enhed, som chefen eller lederen har personaleansvar for.
Nedarvningsprincippet sikrer at chefer og ledere kan tilgå personalesager for eget personale, idet det forudsættes at personalesager udplaceres i de afdelinger hvor medarbejderne er ansat. HR-afdelingen kan tilgå personalesager i hele organisationen.

Direktion

Dataklassifikation HØJ

Anvendelse

Sættes på sager forbeholdt direktionen.

Tildeling

Tildeles medlemmer af direktionen og efter anmodning dens tilknyttede sekretærer.

Tilknytning:

Tilknyttes altid på niveau "Aabenraa Kommune".

Chef
Dataklassifikation HØJ
Anvendelse
Sættes på sager, der har ledelsesmæssig karakter.
Tildeling
Adgangskoden tildeles direktionen, afdelingsledere og evt. gruppeledere.
Tilknytning
Adgangskoden tilknyttes altid lederens "egen afdeling" i Acadrestrukturen.
Nedarvningsprincippet sikrer, at sager beskyttet med adgangskoden "Chef" kun kan ses af afdelingslederen og evt. gruppeledere i den afdeling sagen er placeret, samt af afdelingsledere i overliggende afdelinger. Adgangen til ledelsessager følger kompetencestrukturen.

Beredskabssag
Dataklassifikation HØJ
Anvendelse
Anvendes på sager, der oprettes eller overføres til det fælleskommunale beredskab. Adgangskoden forhindrer centraladministrationen og øvrige administrative enheders adgang til de beredskabssager, der omhandler adgang til og adgangssikring af bygninger.
Tildeling
Tildeles kun medarbejdere i beredskabet.
Tilknytning
Tilknyttes altid beredskabet.

Entreprenørsag
Dataklassifikation HØJ
Anvendelse
Anvendes på sager, der oprettes eller overføres til enheder under den kommunale kontraktstyrede entreprenørvirksomhed. Adgangskoden forhindrer centraladministrationen og øvrige administrative enheders adgang til informationer, der kun vedrører entreprenørvirksomheden (konkurrencehensyn).
Tildeling
Tildeles medarbejderne i den kontraktstyrede entreprenørvirksomhed samt direktøren under hvis kompetence virksomheden fungerer.
Tilknytning
Tilknyttes altid den kommunale kontraktstyrede entreprenørvirksomhed.

Fortrolig
Dataklassifikation HØJ
Anvendelse
"Fortrolig" er en ad hoc adgangskode, som f.eks. kan anvendes ved sager om udbud, køb og salg af ejendomme, eller andre lignende sager, hvor kommunen har en forpligtelse til at informationer kun kommer til få medarbejderes kendskab.
Tildeling
Tildeles ad hoc af IT-administrationen efter indstilling fra afdelingslederne.
På baggrund af indstillingen vurderer IT-administrationen, om tildelingen er hensigtsmæssig. Tildelingen kan i visse tilfælde nægtes, idet det skal undgås at der opstår uhensigtsmæssige dataadgange, hvor "nedarvningsprincippet" gør det muligt for uvedkommende at se underliggende afdelingers dokumenter påført samme adgangskode.
Tilknytning
Tilknyttes som udgangspunkt kun på afdelings-, eller gruppeniveau.

Øvrige adgangskoder
Dataklassifikation HØJ
Anvendelse
Hvis der er et behov for at begrænse sager til en delmængde af medarbejdere, vil dette være muligt ved hjælp af tildelingen af adgangskoder til enkelte brugere. Adgangskoderne anvendes, hvor kommunen har en forpligtelse til at informationer kun kommer til få medarbejderes kendskab.

Tildeling
Tildeles ad hoc af IT-administrationen efter indstilling fra afdelingslederne.
På baggrund af indstillingen vurderer IT-administrationen, om tildelingen er hensigtsmæssig. Tildelingen kan i visse tilfælde nægtes, idet det skal undgås at der opstår uhensigtsmæssige dataadgange, hvor "nedarvningsprincippet" gør det muligt for uvedkommende at se underliggende afdelingers dokumenter påført samme adgangskode.
Tilknytning
Tilknyttes som udgangspunkt kun på afdelings-, eller gruppeniveau.

Dataklassifikation 2 - Mellem

Borgersag

Dataklassifikation MELLEM
Anvendelse
Anvendes på personsager, hvor CPR-nummeret er sagsidentifikation, hvor sagen ikke indeholder oplysninger af ren privat karakter, (persondatalovens § 6.1), sager om økonomi, bopæl m.v.
Tildeling
Tildeles medarbejdere, der arbejder med den pågældende sagstype.
Automatik: Når en medarbejder er tildelt adgangskoden "Borgersag" foreslås denne automatisk af systemet, sat på sager, der oprettes med sagstypen "Borgersag". Se afsnittet "Sagstyper".
Tilknytning
For medarbejdere i centraladministrationen tilknyttes adgangskoden niveau "Aabenraa Kommune".
Der kan efter anmodning tildeles adgangskoden på andre niveauer i Acadrestrukturen til medarbejdere, der arbejder med pågældende sagstype.
For medarbejdere uden for centraladministrationen tilknyttes adgangskoden den afdeling i Acadrestrukturen, hvor medarbejderen organisatorisk er placeret (hvor primærrollen er tilknyttet).

Dataklassifikation 3 - Lav

Centraladministration

Dataklassifikation LAV
Anvendelse
Anvendes på alle sager i den centrale administration, der ikke adgangssikres med en af de øvrige adgangskoder.
Tildeling
Tildeles alle medarbejdere, der arbejder med sager, der klassificeres efter klassifikationsniveau 3 (i princippet alle medarbejdere).
Adgangskoden tilknyttes dog efter 2 forskellige regler, afhængigt af om man arbejder i centraladministrationen eller på en institution.
Tilknytning
For medarbejdere i centraladministrationen tilknyttes adgangskoden altid på niveau "Aabenraa Kommune".
For medarbejdere på institutioner tilknyttes adgangskoden den aktuelle institution.

Sagstyper

Borgersag (BGSAG)
Sager af denne type påføres automatisk adgangskoden "Borgersag" ved oprettelse, såfremt brugeren er tildelt denne.

Personalesag (PERSAG)
Sager af denne type påføres automatisk adgangskoden "Personalesag" ved oprettelse, såfremt brugeren er tildelt denne.

Emnesag (EMSAG)
Sager af denne type påføres automatisk adgangskoden "Centraladministration" ved oprettelse, såfremt brugeren er tildelt denne.

Ejendomssag (EJSAG)
Sager af denne type påføres automatisk adgangskoden "Centraladministration" ved oprettelse, såfremt brugeren er tildelt denne.

Børn og Ungesag (BUSAG)
Sager af denne type påføres automatisk adgangskoden "Særlig Borgersag" ved oprettelse, såfremt brugeren er tildelt disse.

Skanning

Acadrestrukturen anvendes ved distribution af indskannet post.

Principper for distribution af indskannet post.

Indskannet post distribueres til brugerne og placeres i Acadrestrukturen efter 2 principper:

1. Til den modtagende Acadrebruger

Når posten distribueres direkte til en brugers postkasse "Dagens post", vises posten kun i denne brugers postkasse i Acadre.
Ulempen ved denne form for distribution er, at ingen andre brugere i systemet vil kunne se eller registrere denne post. Heller ikke en afdelingsleder. Derfor er der indført en regel, der automatisk synliggør posten til afdelingen efter 14 dage.

2. Til den modtagende afdeling i Acadrestrukturen

Her kan posten ses og behandles af alle medarbejdere, der er tildelt en rolle i den administrative enhed, som posten distribueres til.
Denne form for distribution sikrer, at flere medarbejdere kan se et indskannet dokument, og handle på det, såfremt det er nødvendigt.
Store afdelinger, der modtager meget post, kan med fordel opdeles i arbejdsgrupper (underliggende administrative enheder) i Acadrestrukturen.
Afdelingsledere vil i visse tilfælde have brug for at kunne se post for flere underliggende afdelinger, for at kunne følge med i, om der er post, der mangler at blive journaliseret. I sådanne tilfælde skal lederen tilknyttes alle de aktuelle administrative enheder som sagsbehandler (sekundære roller).

Postmodtagelse og skanning

Kvalitetssikring

Sagsbehandleren har pligt til at sikre sig, at alle skannede sider og bilag i dokumentet kan læses. Hvis det ikke er tilfældet, skal skanningsfunktionen kontaktes via mail, og dokumentet omskannes.

Bevisværdi (retsbærende dokumenter)

For at sikre de skannede dokumenters autenticitet og integritet skal der være personmæssig adskillelse mellem kvalitetssikringen og skanningen. Samme medarbejder må ikke stå for såvel skanning som kvalitetskontrol af samme dokument.
Originale papirdokumenter, der i sig selv har en høj bevisværdi skal opbevares forsvarligt.
Forvaltningerne skal definere, hvilke originaldokumenter, der har høj bevisværdi.
Dokumenterne skal skannes og opbevares i det papirarkiv, der vil blive opbygget parallelt med det elektroniske arkiv, og det markeres i ESDH-systemet, at originaludgaven forefindes i papirarkivet, med angivelse af fysisk placering.
I papirarkivet skal der tages hensyn til de almindelige krav om genfinding og arkivering.

Registrering af post

Registreringen består af følgende:

- Tilknytning af dokumentet til en ny eller eksisterende sag.
- Registrering af styringsoplysninger, eksempelvis aktiviteter, erindringsdato etc.

Fordeling af:

De skannede dokumenter

Når posten er skannet ses der på "Dagens Post" for afdelingen.

Papirdokumenter efter skanning

Skannet post - Efter skanning tages de dokumenter fra, som enten skal bruges af sagsbehandleren eller skal gives tilbage til ejeren efter sagsbehandlingen.
Der er her primært tale om retsbærende dokumenter.
Retsbærende dokumenter er dokumenter, der i originalt papirformat tillægger en person eller en myndighed en ret.

Det kan f.eks. være:

- Kørekort
- Skøder

- Pantebreve
- Kontrakter
- Policer
- Bidragsdokumenter
- Attester

De nævnte dokumenter fordeles til de enkelte sagsbehandlere/afdelinger/forvaltninger.
De resterende dokumenter opbevares i datoorden, med henblik på en evt. omskanning.
Ikke skannet eller delvist skannet post – materiale, som af praktiske årsager enten ikke er skannet, eller kun delvist er skannet, omdeles til den ansvarlige medarbejder, som har pligt til at opbevare/arkivere dette.

Adgangsgrupper

Adgangsgrupper anvendes til at give "gæsteadgang" til sager beskyttet af adgangskoder (underforstået, at "gæsten" sædvanligvis ikke arbejder med, eller har adgang til den konkrete sag eller sagstype).

Gæsteadgang til en sag ved hjælp af 3 handlinger i Acadre

Det er kun sager beskyttet af en adgangskode, der kan være behov for at give gæsteadgang til.
Gæsteadgang oprettes af en medarbejder med adgang til den sag, der ønskes gæsteadgang til gennem "Adgangsgrupper".

Der skal udføres 3 handlinger i Acadre:

1. Medarbejderen skal vurdere om "gæsten/gæsterne" bør have adgang til sagen, og i givet fald, hvor længe der skal gives adgang.
   Medarbejderen opretter derefter en adgangsgruppe, og knytter den til sagen (adgangsgruppen kan efter behov knyttes til flere sager).
   Medarbejderen kan tidsbegrænse adgangen til adgangsgruppen (og dermed tidsbegrænse adgang til sagen).

2. Medarbejderen tilføjer den eller de kolleger, som skal tildeles "Gæsteadgang", til adgangsgruppen.
   Eksisterer der allerede en adgangsgruppe, anvendt ved en tilsvarende "Gæsteadgang", kan denne adgangsgruppe genanvendes. Men vær her sikker på at personkredsen i adgangsgruppen passer til formålet.

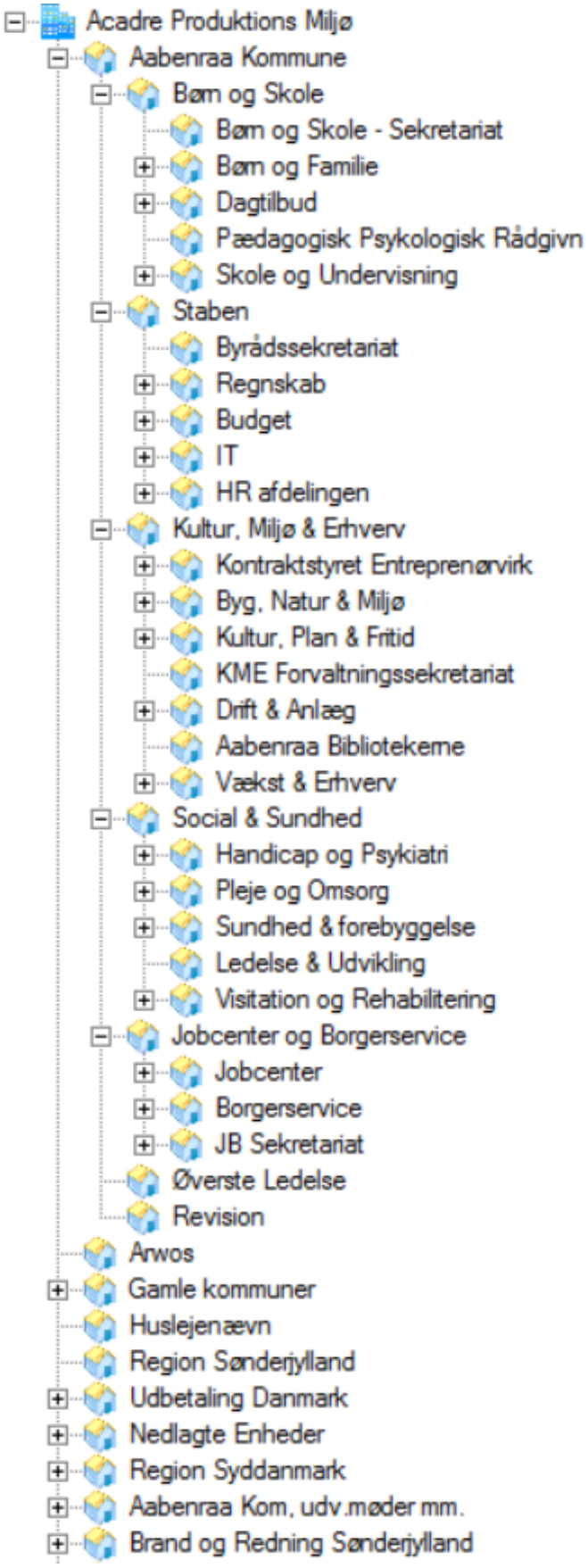
3. Medarbejderen sender herefter en anmodning til IT-afdelingen, om at "Godkende" den eller de kolleger, der ønsker "Gæsteadgangen" til sagens "Adgangskode". (Henvendelse til IT-afdelingen sker gennem Helpdesksystemet).
   Når IT-afdelingen gennemfører "Godkendelsen" af adgangskoden, er der åbnet for gæsteadgangen.
   BEMÆRK at IT-afdelingens "**Godkendelse**" af en medarbejder til en adgangskode, kun giver medarbejderen adgang til de sager, der er beskyttet med adgangskoden **gennem "Adgangsgrupper"**.
   Den direkte adgang til at anvende en adgangskode kræver en "Tildeling" (autorisation), som beskrevet i afsnittet "Roller og Adgangskoder".

Ikrafttrædelse

Acadre Sikkerhedsindretning for Aabenraa Kommune blev godkendt i Den Digitale Styregruppe den 20. februar 2017.

IT-Digitalisering
ESDH-teamet
Lokale 114
Januar 2017

Bilag 1 - Acadre organisationsstruktur - 01-2017



Bilag 2 - Procedure for håndtering af sager og dokumenter ved fratrædelse

Baggrund
I forbindelse med at en medarbejder (NN) fratræder sin stilling ved Aabenraa Kommune, skal den respektive leder tage stilling til de sager i ESDH-systemet Acadre, som NN er sagsansvarlig for. Ansvarskompetencen kan uddelegeres til den ESDH-ansvarlige/superbruger.

Procedure:
I IT-Helpdesk opretter lederen eller de af lederen bemyndigede medarbejdere en proces, der fratræder eller rokerer NN. IT-Helpdesk genererer en delopgave til den ESDH-ansvarlige/superbruger, der skal sikre at NN får tjekket udtjekkede dokumenter ind, og at der tages stilling til afslutning af sager samt registrering af, hvem der skal overtage aktive sager. Processen kan *ikke* afsluttes før denne registrering er afsluttet.

I det følgende skelnes mellem sager, dokumenter og (journal)notater.

Sager
En Acadresags tilstand eller sagsstatus er defineret som en af følgende:
A - Afsluttet
B - Under behandling
P - Passiv

1. Afsluttede sager (A) må ikke overdrages til en anden sagsbehandler.
Det vil fortsat være relevant at kunne se, hvem der behandlede sagen, da den verserede. I den forbindelse er det irrelevant, om vedkommende stadig er ansat ved Aabenraa Kommune. Det er dels vigtigt, hvis der opstår tvivl om sagens fakta, ligesom det er vigtigt, hvis der skulle opstå tvistigheder af juridisk art i en sag. I en sådan situation er det yderst relevant for kommunen at kunne dokumentere, hvilken medarbejder der har været sagsbehandler.
Der kan være behov for at genåbne en afsluttet sag. Man må imidlertid ikke genåbne en sag med henblik på at skifte sagsbehandler. En genåbning af sagen skal være indholdsmæssigt begrundet. Sager der har været afsluttet i mere end 6 måneder bør dog ikke genåbnes, idet det ikke med sikkerhed kan vides, hvilke forudsætninger der i sin tid har været årsag til at sagen blev afsluttet. I stedet for, bør der oprettes en ny sag med en henvisning til den tidligere sag.

2. Sager under behandling (B) og passive sager (P) skal gennemgås inden NN rejser.
Afdelingens ESDH-ansvarlige/superbruger trækker en rapport over de sager NN er sagsansvarlig for. Sammen med afdelingens ledelse gennemgås sagerne. Det afklares, hvilke af sagerne der bør afsluttes. Når en sag afsluttes inden NN fratræder, forbliver NN registeret som sagsansvarlig.
NN's sager, der efter gennemgangen af sagerne har sagsstatus B - Under behandling eller til P - Passiv overdages til en ny sagsansvarlig. Den ESDH-ansvarlige/superbrugeren kan være behjælpelig med at overdrage et større antal sager. Acadre sender via Outlook en mail til den nye sagsansvarlige med oplysning om, hvilken sag pågældende har fået ansvar for. Overdragelsen af en sag bør så vidt muligt være ledsaget af en orientering om sagens baggrund og indholdsmæssige status fra NN/afdelingens ledelse.

Dokumenter
Alle dokumenter, der er oprettet eller journaliseret i Acadre forbliver journaliseret under den sagsbehandler, der har skrevet dem. D.v.s., at selvom en sag afsluttes eller overdrages til en anden sagsansvarlig, så vil den sagsbehandler, der har skrevet dokumentet, fremgå af dokumentprofilen.
Det skyldes, at det fortsat vil være relevant at kunne se, hvem der skrevet dokumentet. I den forbindelse er det irrelevant, om vedkommende stadig er ansat ved Aabenraa Kommune. Det er dels vigtigt, hvis der opstår tvivl om dokumentets fakta, ligesom det er vigtigt, hvis der skulle opstå tvistigheder af juridisk art.
Kun i situationer, hvor f.eks. et udkast til et brev eller notat skrives færdig af en anden sagsbehandler, bør navnet på den dokumentansvarlige ændres, fordi det her vil være den nye sagsbehandler, der færdiggør dokumentet.

(Journal)Notater
Alle notater der skrives via Acadres notatfunktion (telefon- og journalnotater) forbliver journaliseret under den sagsbehandler, der har skrevet notatet. D.v.s., at selvom en sag afsluttes eller overdrages til en anden sagsansvarlig, så skal det fortsat fremgå af journal- eller telefonnotatet, hvem der har skrevet notatet.
På samme måde som ved dokumenterne, vil det fortsat være relevant at kunne se, hvem der har skrevet notatet. I den forbindelse er det irrelevant, om vedkommende stadig er ansat ved Aabenraa Kommune.

Bilag 3 - Undtagelser fra sikkerhedsindretningen

~~**Genåbning af sager**~~

~~Som beskrevet i Sikkerhedsindretning for Aabenraa Kommune, er det kun administratorer, der kan genåbne sager i hele organisationen. Administratorer består af ESDH-teamet i IT-afdelingen.~~

~~Der er lavet enkelte undtagelser fra denne regel, og rettighederne er tildelt følgende superbrugere:~~

- ~~Tora Johanne Busch Djernæs (TJD) i Kultur, Miljø og Erhverv~~
- ~~Joan Martinussen (JMAR) i Jobcenter og Borgerservice~~

~~**Kun sager under Aabenraa Kommune og i eget forvaltningsområde må genåbnes af de udvalgte superbrugere.**~~

16. juni 2023 - Acadre Sikkerhedsindretning, bilag 3, første afsnit "Genåbning af sager" ændres til:

Genåbning af sager og oplåsning af dokumenter

I Acadre Sikkerhedsindretning for Aabenraa Kommune fremgår det at det kun er administratorer (med ganske få undtagelser), der har adgang til at genåbne sager, og at adgangen til at oplåse dokumenter er begrænset i Acadre, så det kun er administratorer og superbrugere, der har denne mulighed.
Når der er behov for, enten at få genåbnet en sag eller låst et dokument op, skal der oprettes en opgave i helpdesksystemet, hvilket ofte forhaler færdiggørelse af sager/arbejdsopgaver.
I modsætning til Acadre WEB-klient, dannes der i Acadre CM ikke automatisk en ny version, når et dokument ændres. Man kan således ikke se, hvilke ændringer der er foretaget af de forskellige sagsbehandlere, som har haft dokumentet åbnet.
Dette er, i den nuværende sikkerhedsindretning, blandt andet en af begrundelserne for, at kun få udvalgte medarbejdere har denne mulighed.
Når alle medarbejdere er overgået til WEB-klienten, vil der blive åbnet op for, at den enkelte sagsbehandler selv kan låse dokumenter op og genåbne sager, da alle arbejdsgange fremgår tydeligt af historikken.
Indtil Acadre CM er udfaset, og alle medarbejdere er overgået til WEB-klienten, er det besluttet at løsne lidt op, så udvalgte nøglepersoner også får mulighed for at genåbne sager og låse dokumenter op.
Adgangen skal bestilles via processkema af nærmeste leder eller hertil godkendt medarbejder.
Indtil Acadre CM er udfaset, skal de udvalgte nøglepersoner dokumentere, hvad der genåbnes og låses op.

Ændring af autoprofil

Der er oprettet en speciel rolle til superbrugere/medarbejdere, der har behov for at kunne administrere og oprette autoprofiler til øvrige medarbejdere i forvaltningen.
Funktionen kan tildeles efter indmelding i helpdesksystemet.

Bilag 4 - Rollerettigheder i Acadre

		De med "*" markerede roller er oprettet af ESDH-teamet													
Roller i CM	**Indstillingsmuligheder**	Brugeradministration *	Dagsordensamler	Fuld Rettighed	Genåbne sag og Slet papirkurv *	Journalmedarbejder	Læser	Ret til ændring af autoprofil *	Sagsbehandler	Sagsbehandler-Begrænset *	Slet Dagens Post *	Superbruger	Workflowadministrator	X-Administrator	Z-Adm - GeoEnviron *
Annuller Check-ud	0 = Ingen ret														
	1 = Ret til at annullere check-ud på dokumenter du selv har checket ud - med advarsel								X			X			
	2 = Ret til at annullere check-ud på dokumenter du selv har checket ud - uden advarsel														
	3 = Ret til at annullere check-ud på alle dokumenter, som brugeren har redigeringsrettighed til - med advarsel													X	X
	4 = Ret til at annullere check-ud på alle dokumenter, som brugeren har redigeringsrettighed til - uden advarsel														
Daily Mail access private level	0 = Ingen ret til at se andre brugeres fortrolige post														
	1 = Ret til at se andre brugeres fortrolige post i brugerens primære administrative enhed														
	2 = Ret til at se andre brugeres fortrolige post i de administrative enheder, hvor brugeren har en rolle														
	3 = Ret til at se andre brugeres fortrolige post i de administrative enheder og underenheder, hvor brugeren har en rolle														
Flytte journalpost	0 = Ingen ret til at flytte journalposter														
	1 = Ret til at flytte journalposter mellem sager for hvilke bruger selv er sagsansvarlig														
	2 = Ret til at flytte journalposter mellem sager inden for den til rollen knyttede administrative enhed									X				X	X
	3 = Ret til at flytte journalposter inden for hele organisationen			X		X			X			X			
Ledelse (skabeloncenter)	0 = Ingen ret til skabeloncenteret														
	1 = Ret til skabeloncenteret			X					X	X		X		X	
Oplåse dokumenter	0 = Må ikke oplåse dokumenter														
	1 = Må gerne oplåse dokumenter		X	X		X						X		X	X
Oprette journalpost for internt dokument	0 = Ingen ret til at journalisere internt producerede dokumenter														
	1 = Ret til at journalisere internt producerede dokumenter med bruger selv som ansvarlig på sager hvor bruger optræder enten som sagsansvarlig eller som afsender/modtager på eksisterende journaliseret dokument					X									
	2 = Ret til at journalisere internt producerede dokumenter med bruger selv som ansvarlig														
	3 = Ret til at journalisere internt producerede dokumenter med sagsbehandler fra den til rollen knyttede administrative enhed som ansvarlig									X				X	X
	4 = Ret til at journalisere internt producerede dokumenter uden begrænsning		X	X					X			X			
Oprette sag	0 = Ingen ret til at oprette sager														
	1 = Ret til at oprette sager med bruger selv som sagsansvarlig inden for den til rollen knyttede administrative enhed													X	
	2 = Ret til at oprette sager inden for den til rollen knyttede administrative enhed					X				X					X
	3 = Ret til at oprette sager inden for hele organisationen			X					X			X			
Redigere sager	0 = Ingen ret til at redigere														
	1 = Rediger egne sager														
	2 = Redigere sager i samme administrative enhed									X					
	3 = Ret til at redigere alle sager		X	X		X			X			X		X	X
Revoke daily mail reservation	0 = Ingen ret til at annullere Dagens Post														
	1 = Ret til at annullere Dagens Post										X				
Slette i dagens post	0 = Må ikke slette														
	1 = Må gerne slette										X				
Slet/Gendan sager	0 = Ingen ret til gendan/slet														
	1 = Gendan/Slet hvis sagsansvarlig					X			X	X		X			
	2 = Gendan/slet hvis sagen indenfor samme administrative enhed														
	3 = Fuld ret til gendan/slet overalt i organisationen			X										X	
Systemadministrator	0 = Ikke systemadministrator på systemet														
	1 = Har ret til at administrere brugere og afdelinger	X			X									X	
	2 = Er administrator på systemet														
Søg i kontaktrelationer	0 = Ingen ret til at søge i kontaktrelationer														
	1 = Ret til at søge i kontaktrelationer		X	X		X	X		X	X		X		X	X
Søge	0 = Ingen ret til at søge		X												
	1 = Ret til at søge					X	X		X	X		X		X	X
Søge i P-data	0 = Ingen ret til at søge i P-Data														
	1 = Ret til at søge i P-Data			X		X			X	X		X		X	X
Workflowadministrator	0 = Ingen ret til at administrere workflows														
	1 = Ret til at administrere workflows												X		
Ændre adgangsbegrænsninger	0 = Ingen ret til at ændre adgangsbegrænsninger (dvs adgangskode, adgangsgruppe, afgraderingskode, mm)														
	1 = Ret til at ændre adgangsbegrænsninger på sager, dokumenter, osv for hvilke bruger selv er ansvarlig														
	2 = Som 1 plus journalposter tilhørende sager for hvilke bruger er ansvarlig														
	3 = Som 2 plus journalposter tilhørende sager for hvilke ansvarlig tilhører den til rollen knyttede administrative enhed									X					
	4 = Ingen begrænsninger			X		X			X			X		X	X
Ændre autoprofiler	0 = Ingen ret til at ændre														
	1 = Ret til at ændre							X				X		X	
Ændre lynsøgninger	0 = Ingen ret til at ændre lynsøgninger														
	1 = Ret til at ændre lynsøgninger											X		X	
Ændre sagsansvarlig	0 = Ingen ret til at ændre sagsansvarlig														
	1 = Ret til at ændre sagsansvarlig inden for den til rollen knyttede administrative enhed									X				X	X
	2 = Ret til at ændre sagsansvarlig inden for hele organisationen			X		X			X			X			
Ændre sagsstatus	0 = Ingen ret til at ændre sagsstatus														
	1 = Ret til at ændre sagsstatus på sager for hvilke bruger selv er ansvarlig														
	3 = Som 1 plus sager hvis sagsansvarlige tilhører den til rollen knyttede administrative enhed														
	4 = Ingen begrænsninger			X					X	X		X		X	X