Notat

Vedrørende: Retningslinie for adgangsstyring og rettigheder i SBSYS
Sagsnavn: Retningslinie for sikkerhed og rettigheder i SBSYS
Sagsnummer: 85.15.00-A26-3-18
Skrevet af: Majbrit Jøns
E-mail: majbrit.jons@randers.dk
Forvaltning: IT og digitalisering

Indledning

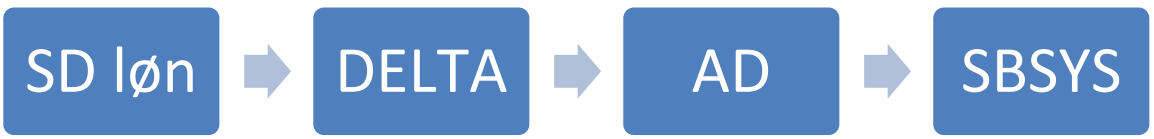
ESDH ansvarlig og Delta ansvarlig fra IT og digitalisering har i samarbejde med Stabschefen og Chefjuristen udarbejdet principperne for sikkerhedsstrukturen i SBSYS i foråret 2018.
Formålet har været at sikre at adgangsstyring og rettigheder i SBSYS følger reglerne i Databeskyttelsesforordningen/databeskyttelsesloven. Endvidere er der lagt vægt på reglerne i Forvaltningsloven omkring tilgængelighed og videregivelse af personlige oplysninger.

Brugeroprettelse i SBSYS

SBSYS er kommunes generelle ESDH system og dermed systemet, hvor medarbejderne skal håndtere journalisreingspligtige data, der ikke kan håndteres i andre fagsystemer. Derfor bliver alle ansatte oprettet i SBSYS, med undtagelser af;

- Brugere, der ikke anvender IT
- Udførende personale på ældrecentrene
- Ikke-administrativt personale på folke- og specialskolerne

Brugeroprettelse og ændringer til SBSYS foregår automatisk ved at en bruger bliver oprettet eller skifter funktion/ansættelsessted, oplysninger overføres dagligt til Delta (Kommunes IdM) hvor roller og sikkerhed tildeles, hver 2. time synkroniseres oplysningerne til AD (Active directory) hvor der tilføres brugerlogon og adgange til systemer og drev administres. Brugerdata fra AD synkroniseres over i SBSYS hver 2. time



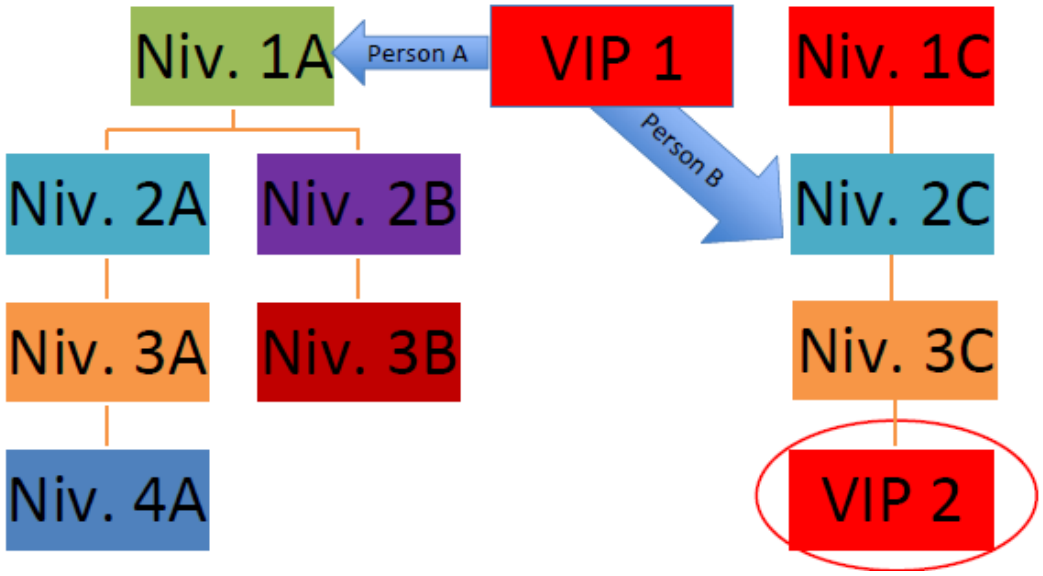
Figur 1 Viser dataflow for brugeroprettelse/brugerændringer

Overordende principper for sikkerhedsstrukturen

Nedenstående figur, viser principperne for adgang til sager i SBSYS, skal læses på følgende måde at niv. 1A har adgang til alle sager, der ligger på de underliggende niveauer, men vil ikke have adgang til sager der i C søjlen.

Niv. 2A har adgang til alle sager, der ligger under (niv. 3A og 4A), men vil ikke have adgang til sager der ligger i niv. 2B og 3B.

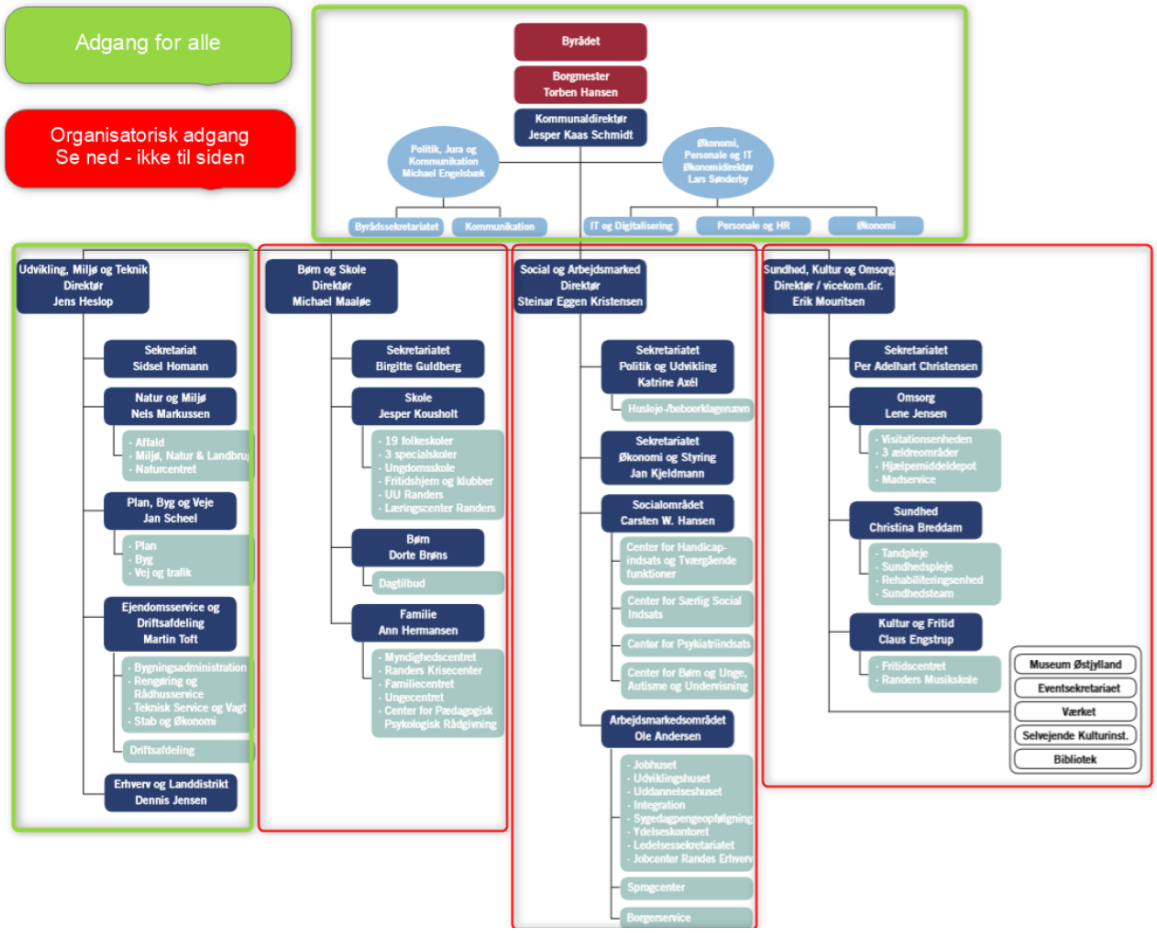
Med VIP grupper, er det muligt at håndtere afgræsning af områder eller giver adgang til udvalgte personer på tværs af områder.



Figur 2 Princip for sikkerhedsstruktur

Den konkrete udmøntning af sikkerhedsstrukturen pr forvalning er aftalt med sekretariatschefen og SBSYS kontaktsuperbrugeren for de enkelte forvaltninger.

Stabene og Udvikling, Miljø og Teknik har valg at alle sagerne i princippet er 'Abne for alle'
Social- og Arbejdmarked, Sundhed, Kultur og Omsorg og Børn og Skole har valg 'Se ned – ikke til siden' som lilustreret i figur 2



Figur 3 Konkret udmøntning af sikkerhed på Randers organisationen

Det er områderne/enhederne/afdelingerne eget ansvar at kontakte SBSYS teamet, hvis det viser sig at den organisatoriske sikkerhed ikke er optimal iforhold til videndelen og/eller afskærmning af personhenførebare data.

Ændringer i organiseringen

Kontaktsuperbrugerne i forvaltningerne har ansvaret for at melde større organisatoriske ændringer ind. Der tages stilling til om sagsstruktur/-sikkerhed skal ændres, når der justeres i opgaver og organisering i forvaltningerne.

VIP adgangslister

Som tidligere skrevet bliver der efter behov oprette "VIP gruppe" adgange. Det er særskilte oprettede sikkerhedsgrupper for at efterleve reglerne i Databeskyttelsesforordningen og Databeskyttelsesloven – f.eks. Kontrolgruppen i Borgerservice.

Ved etablering af sikkerhedsgrupperne er der særlig fokus på adgang og indsigt i sager med følsomme og fortrolige personoplysninger, så adgangen til disse begrænses til de brugere/enheder, der har

behov for adgangen. Endvidere har der været fokus på Forvaltningslovens § 32, som siger: *Den, der virker inden for den offentlige forvaltning, må ikke i den forbindelse skaffe sig fortrolige oplysninger, som ikke er af betydning for udførelsen af den pågældendes opgaver.*

Manuel redigering af adgangslister på sager

Det er muligt manuelt at redigere i adgangslisten på sagen, hvilket kræver manuel vedligeholdelse på den enkelte sag og dermed er det den enkelte sagsbehandlers ansvar at vedligeholde adgangslisten.

Vedligehold af sikkerhed

Hovedparten af brugervedligholdelse foregår fra fra SD Løn, da adgangen til SBSYS styres udfra om den ansatte er aktiv i SD løn, hvilke afdelingen den ansatte er tilknyttet, dermed håndteres skift af ansættelsessted ligeledes i SD løn.

Hvis brugeren er tilknyttet VIP sikkerhedsgrupper er det den ansvarlige for VIP gruppen, der via IT support skal melde ændringen ind

Brugerroller i SBSYS

Der er følgende brugerroller i SBSYS

- Administrator
- Bruger (Tilknyttet alle brugere, er nødvendige for synkronisering fra AD)
- Dagsordensansvarlig
- Sagsbehandler (Tilknyttet alle brugere, er nødvendig for synkronisering fra AD)
- Skabelonadminstrator

Administrator

En administrator har bl.a. rettigheder til at se alle sager oprettet i SBSYS, foretage brugeroprettelser, oprette sikkerhedsgrupper og foretage generel systemvedligeholdelse
Der er 5 administrator fra IT herunder, 2 fra ESDH teamet, der har administratorrollen, samt nogle servicebrugere – integrationer fra andre systemer fx SBSIP.

Bruger/sagsbehandler

De resterende brugere i SBSYS er som udgangspunkt oprettet med standardsikkerhed, hvilket vil sige, at de har adgang til de sager, følgende de overstående principper for adgang i SBSYS.

Dagsordensanvarlige

Når en dagsordensansvarlig har adgang til et udvalg via dagsordensadministration, har brugeren adgang til sagen også selv om brugeren ikke står på sagens adgangsliste. Det er den ansvarlige for udvalget, der administrer adgangen på udvalgene.

Skabelonadministrator

Giver ikke udvidet sagsadgang. Brugere med roller har mulighed for at oprette sagskabeloner og kladdeskabeloner.

Superbruger

Giver ikke udvidet sagsadgang. Brugere med roller har udvidet funktionsmulighed som af afslutte kladderedigering for andre.

Systembrugere til SBSYS

Der findes forskellige systembrugere som bruges til integration til SBSYS og for at databasen kan få data ud og ind.
Systrem brugere bruges til eks. digital post opsætning i systemet og aflevering til eboks kø/sbsip, integration til systemer ind til SBSYS, og andre services som skal kører i databasen.
Systembrugere anvendes til integration til og for at databasen fungerer, der logges ikke ind med disse brugere.

Logning

Jf. kommunens informationssikkerhedsregler er det den enkelte leders og evt. systemejeren, der skal sikrer, at oplysninger ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, det kan sikre ved at foretage stikprøver, da aktivitet i SBSYS logges.

Løbende evaluering

En gang om året foretages evaluering af;

- VIP lister. Den ansvarlige for listen får fremsendt brugerlisten og skal godkende den er gældende
- Sikkerhedsadgange for områderne. Kontaktsuperbrugeren for forvaltningen gennemgår og godkender forvaltningens sikkerhedsmodel
- Adgange på udvalg. Den ansvarlige for udvalget skal godkende at adgangslisten er gældende