Retningslinjer for brugerautorisationer

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
1.1	06-05-2021	Mindre redaktionelle rettelser	Sikkerhedsrådgiver	Sikkerhedsteam
1.2	30-05-2022	Afsnit om administratorbrugere og Kontrolenheden tilføjet	Sikkerhedsrådgiver	Sikkerhedsteam
1.3	23-01-2025	Mindre redaktionelle rettelser samt tilføjelse af afsnit om kontrol af administratorer	Sikkerhedsrådgiver	Sikkerhedsteam

Formål

Disse retningslinjer har til formål at sikre, at brugerautorisationer til alle it-systemer, som indeholder personoplysninger samt almindelige eller følsomme forretningsoplysninger, håndteres korrekt efter databeskyttelsesforordningens artikel 32, stk. 1, som pålægger den dataansvarlige at gennemføre passende tekniske og organisatoriske foranstaltninger.

Offentligt ansatte må kun behandle personoplysninger, som de har et arbejdsbetinget behov for at behandle. Den enkelte autorisation må derfor kun give ret til at behandle oplysninger, der er relevante og nødvendige for medarbejderens arbejde. Dette gælder både i forhold til tildeling og fratagelse af adgange samt kontrol af disse.

Logisk adgangsstyring

Den overordnede logiske adgangsstyring til it-ressourcer kan kun ske via Jammerbugt Kommunes administrative it-netværk. Logisk adgangsstyring er organiseret, så ansvaret for tildeling og fratagelse af rettigheder og adgange ligger hos den enkelte leder.

Digitalisering, IT og Borgerservice er udførende og koordinerende i forbindelse med adgangsstyring, ansvarlig for daglige retningslinjer og vejledning i brug af de logiske it-ressourcer. For nogle fagsystemer har systemforvalteren dog ansvaret for brugeradministration.

Administratorbrugere

Udpegede medarbejdere i Digitalisering, IT og Borgerservice er autoriseret til at have administratorrettigheder til de centrale, tværgående it-systemer og netværk. Derudover er udvalgte medarbejdere autoriseret til at have administratorrettigheder til udvalgte systemer. Det gælder typisk for systemforvaltere.

Derudover kan enkelte eksterne samarbejdspartnere opnå administratorrettigheder, hvis det kræves som en del af deres opgaver. Digitalisering, IT og Borgerservice dokumenterer og overvåger adgangen for eksterne brugere med administratorrettigheder.

Central og decentral brugeradministration

I Jammerbugt Kommune findes der to områder for brugerautorisationer:

- Central brugeradministration: Hovedparten af autorisationer på kommunens it-systemer styres centralt. Digitalisering, IT og Borgerservice opretter, ændrer og sletter brugerprofiler på foranledning af nærmeste leder, der opretter en sag hos Servicedesk. Derefter håndterer Servicedesk den konkrete brugeradministration.

- Decentral brugeradministration: For visse it-systemer (f.eks. mindre decentrale systemer, som kun bruges af et specifikt fagområde) gælder det, at systemejer/-forvalter som regel står for brugeradministration.

Ansvar for adgangsstyring og kontrol af adgange
Ansvaret for den daglige adgangsstyring bliver varetaget af på baggrund af følgende procesbeskrivelse:

Ansvarlig	Ansvarsområde
Alle medarbejdere	• Informerer nærmeste leder om behov for adgange til it-systemer.
Ledere med personaleansvar	• Den nærmeste ledelse har det overordnede ansvar for at sikre, at de rette personer/grupper er udpeget og informeret om deres relevante ansvar i forbindelse med adgangsstyringen. • Informerer de ansvarlige for brugeradministration om relevant information i forbindelse med oprettelse/ændring/nedlæggelse af brugere i egen afdeling. • Informerer om login-information til medarbejdere i egen organisation.
Servicedesk (Digitalisering, IT og Borgerservice)	• Sikrer, at medarbejdere er oprettet med de nødvendige/korrekte adgange til it-systemer i henhold til den indsendte anmodning fra leder. • Registrerer/kvalificerer nye behov for oprettelse/ændring/nedlæggelse af roller. Derudover indhenter Servicedesk godkendelse fra rolleejerne. • Udfører ændringer i roller. • Bistår med udtræk af brugere i centralt administrerede it-systemer, som kan anvendes til at udføre kontroller af brugere.
Systemejer	• Udarbejder procedure for brugerautorisation og kontrol ved brug af kommunens skabelon. • Sikrer, at medarbejdere er oprettet med de nødvendige/korrekte adgange til it-systemer i henhold til den indsendte anmodning fra leder. • Gennemfører jævnlige kontroller af brugeradgange til systemer med personoplysninger. • Følger op på fundne risici ved adgangsstyringen (fx hvis der er mangler i systemets tekniske eller organisatoriske sikkerhedsforanstaltninger).

Sådan håndterer systemejer brugerautorisationer
Nedenstående retningslinjer er rettet mod systemejere, hvis ansvar er at sikre adgangsstyring samt føre kontrol med brugerautorisationer i de systemer, de ejer.

Tildeling af autorisationer
Ved tildeling af autorisationer skal der indgå en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til samt en beskrivelse af, hvilke oplysninger brugeren herved autoriseres (godkendes) til at anvende. Herunder skal systemejeren sikre, at der udarbejdes specifikke beskrivelser af forskellige brugerroller.

Dette sker gennem udfyldelse af kommunens tværgående skabelon for 'Procedure for brugerautorisation og kontrol'.

Der må desuden autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver. Systemejeren har ansvaret for at fastlægge særlige retningslinjer for udstedelse af sådanne autorisationer og for inddragelse af dem. Det kan være midlertidige, fx autorisationer til brug ved en årlig revision.

Ændringer og inddragelse af autorisationer

Brugerautorisationer skal løbende holdes ved lige. Hvis en medarbejder fx får nye opgaver og dermed ikke længere varetager samme funktion, skal adgangen ændres og begrænses, så medarbejderen kun kan tilgå relevante personoplysninger. Det samme gælder, hvis en medarbejder stopper. I så fald skal autorisationerne inddrages senest på dagen for ansættelsens ophør. I visse tilfælde kan det vurderes, at autorisationer skal inddrages inden fx ved mistanke om strafbare forhold.

Ændringer og inddragelse sker ved, at den nærmeste leder til den pågældende medarbejder informerer Servicedesk (eller alternativt systemejer/systemforvalter) om, at vedkommende skal have ændret eller frataget specifikke autorisationer, og fra hvilken dato dette skal ske.

Kontrol med brugerautorisationer

Systemejere er forpligtet til at føre kontrol med brugerautorisationer mindst én gang hvert halve år. Kontrollen skal sikre, at de enkelte brugere ikke er autoriseret til anvendelser, som de ikke har behov for i deres jobfunktion. Det er op til systemejeren at vælge, hvordan kontrollen skal gribes an, og sikre, at kontrollen stemmer overens med risikovurderingen af systemet. Det er systemejer, der har initiativet til at foretage kontrollen.

Systemejere skal udfylde en skabelon 'Procedure for brugerautorisation og kontrol' for at sikre, at dokumentationen vedrørende kontrollen lever op til GDPR-kravene. Efter hver udført kontrol noteres resultatet af kontrollen i proceduren. Efter hver kontrol gemmes proceduren i ESDH-systemet.

Det er vigtigt, at proceduren for kontrol af brugere har fokus på administratorers rettigheder. Ofte har administratorer udvidede rettigheder, hvilket medfører en højere konsekvens i tilfælde af misbrug hos netop brugere af denne type. Det anbefales derfor, at it-systemer altid har mindst to administratorer, og at disse administratorer kontrollerer hinandens rettigheder. Det kan eventuelt være systemejeren og systemforvalteren, som kontrollerer hinanden.

Kontrollen kan først udføres, når systemejer har adgang til brugerdata (dvs. hvem har adgang til hvad?). Der kan være forskellige muligheder for at skaffe brugerdata alt afhængig af det enkelte system. Der findes følgende muligheder:

- Systemejer har adgang til brugerdata: Systemejer kan udføre kontrollen ved at lave et udtræk på samtlige brugere og gennemgå deres adgange. Hvis systemet har mange brugere, og opgaven med at gennemgå alle brugere er for tung administrativ, kan systemejeren vælge at udføre kontrollen via en stikprøve.
- Digitalisering, IT og Borgerservice har adgang til brugerdata: I nogle tilfælde vil systemejer ikke selv have mulighed for at lave et udtræk på brugere eller have alternative måder at få overblik over, hvem der har adgang til hvad. Hvis det er

muligt, kan Digitalisering, IT og Borgerservice på anmodning fra systemejer hjælpe systemejeren. Det vil være forskelligt fra system til system, om det er muligt at lave et udtræk på samtlige brugere, eller om det kun er muligt at foretage enkelte stikprøver.

- Leverandøren har adgang til brugerdata: Hvis det ikke er muligt for Digitalisering, Borgerservice og Indkøb at udarbejde udtræk eller foretage opslag på enkelte brugere, kan det være nødvendigt at kontakte leverandøren for at få tilsendt et udtræk.
- Fysisk kontrol med brugeradgange: Endelig vil systemejere ved systemer med ganske få brugere have mulighed for at foretage kontrollen uden et udtræk eller overblik i systemet. Fx kan en systemejer have et system med tre brugere fra egen afdeling. Her kan kontrollen foretages ved at anmode om at se, hvad brugerne har adgang til via deres it-udstyr.

Størrelsen af stikprøvekontroller skal afhænge af it-systemets risikovurdering, og hvilken databehandling der er tale om, fx hvorvidt der indgår databehandling af følsomme og/eller fortrolige personoplysninger, samt hvor store mængde af oplysninger der behandles. Derudover bør systemejer overveje, hvilken sikkerhed der i øvrigt er i systemet, fx to-faktorvalidering, brugerstyring via AD-integration, funktionsadskillelse/jobfunktionsroller, automatisk tilpasning af adgangsrettigheder ved ændringer af ansættelsesforholdet. Hvis der er en høj grad af sikkerhed omkring brugerstyringen i et it-system, kan dette påvirke vurderingen af, hvor omfattende stikprøvekontrollerne bør være. Beslutningen om stikprøvekontrollens størrelse nedfældes i proceduren.