



## Hvordan sikrer vi, at der tages højde for Hovedudvalgets kommentarer ved implementering af Informationssikkerhedspolitikken.

Hovedudvalgs kommentar	Emnet er omhandlet i politikens punkt	Hvordan tænkes det ind i implementeringen	Hvem har ansvaret
<p><b>1. Retningslinjer skal være forståelige og nærværende for medarbejderne</b> Hovedudvalget ønsker, at det skal være anelse mere præcist, når der er beskrivelse af systemer. Altså; Hvad forstår man med systemer, og hvad må man, og hvad må man ikke? Gerne med nogle eksempler.</p>	<p>Dette er ikke beskrevet konkret i politikken.</p>	<p>I dag arbejder IT-kontraktgruppen med udgangspunkt i at risikovurdere IT-løsninger og ikke kun systemer. Vi arbejder aktivt på at ændre forståelsen i organisationen. IT-kontraktgruppens arbejde bliver evalueret i forbindelse med implementering af politikken. Her vil vi tage højde for at få endnu større fokus på, hvordan vi arbejder aktivt med de forskellige begreber..</p>	<p>IT &amp; Digitalisering i samarbejde med DBR</p>
<p><b>2. Sikker opbevaring</b> Der er flere steder i organisationen usikkerhed om, hvad man må opbevare af data i de forskellige systemer. Der er en stor lyst til at sikre en sikker opbevaring af data, så derfor er det vigtigt med klare retningslinjer for, hvor man sikkert kan opbevare data.</p>	<p>Ansvar for data og sikkerhed:  "Det er lederens ansvar at instruere medarbejderne i hvor data må opbevares og behandles samt sikre, at medarbejderne ikke opbevarer private data i kommunens systemer."</p>	<p>Der arbejdes på at skabe et billede af vores systemlandskab, hvor vi kan se, hvilke forretningskritiske procedurer, der kun kan løses ved brug af flere IT-løsninger. Med denne viden, kan vi lave en god proces for, hvornår og hvordan der skal udarbejdes retningslinjer, når en arbejdsangang involverer flere IT-løsninger. Der kan f.eks. være fokus på de udfordringer, der er:</p> <ul style="list-style-type: none"> <li>- Når vi har data flere steder pga. den enkelte løsnings opbygning.</li> <li>- Når vi bruger en IT-løsning, fordi vi forpligtet til det.</li> <li>- Når en arbejdsangang involverer flere afdelinger.</li> </ul>	<p>Centerchefer og ledere i samarbejde med system- og dataejere.  DBR er til rådighed for sparring.</p>
<p><b>3. Forenklede systemer og arbejdsgange</b> Hovedudvalget ønsker et fokus på mængden af systemer, som vi arbejder i og den manglende integration. Der er mange systemer, som kræver mange arbejdsgange at skifte imellem, ligesom man bruger tid på at koordinere mellem systemerne. Forenklede systemer og automatiske integrationer er derfor et stort ønske</p>	<p>I politikens mål:  "Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af IT, der bl.a. gennem digitalisering og integrationer, skal sikre effektive arbejdsgange."</p>	<p>DBR er i dialog med direktionen og chefforum om, hvordan vi håndterer det stigende antal ønsker til at benytte nye IT-løsninger. Der bliver udarbejdet procedurer med en risikobaseret tilgang til, hvordan vi bedst understøtter den digitale udvikling. IT-kontraktgruppen vil som et led i evaluering af sit arbejde bruge disse procedurer og systemlandskabet for at vurdere, hvordan vi bedst muligt kan understøtte udfordringerne ved den store mængde af IT-løsninger. Der bliver bl.a. kigget på hvordan implementeringsprocessen, bedre serviceaftaler samt uddannelse af systemadministratorer og slutbrugere kan effektivisere arbejdsgangene.</p>	<p>Direktionen, Centerchefer, IT &amp; Digitalisering og DBR</p>
<p><b>4. Sikkerhed</b> Det er vigtigt at sikre en sikker opbevaring af borgernes data. Derfor ønskes det, at det er sikres, at vi inden vi køber nye systemer, er indbygget i systemerne, at der er tænkt over datasikkerhed. Sådan at vi kan have tillid til, at data opbevares sikkert.</p>	<p>"Fortrolighed" (hele punktet)  "Forretningssikkerhed og tilgængelighed" (hele punktet)</p>	<p>Dette vurderes af IT-kontraktgruppen en live-fremvisning af leverandørens teknikere. Her deltager medarbejdere, som skal benytte løsningen. IT-kontraktgruppen vurderer om løsningen er teknisk sikker og kan overholde GDPRs krav til borgernes rettigheder. Fagområdet har ansvaret for implementeringen, herunder, hvordan medarbejderne bliver uddannet inden løsningen tages i brug. IT-kontraktgruppen vil vurdere, hvordan vi ud fra en risikobaseret tilgang kan understøtte fagområdet yderligere i forbindelse med godkendelse af løsningen og f.eks. gøre implementeringsplanen til en del af gennemgangen.</p>	<p>Direktionen, Centerchefer (systemejere), IT &amp; Digitalisering og DBR.</p>

