Plan- og
Landdistriktsstyrelsen

Carsten Niebuhrs Gade 43
1577 København V
www.plst.dk
Telefon 3330 7010
e-mail plst@plst.dk
Sagsnr.
2023 - 6918
Doknr.
202685
Dato.
30.05.24

Retningslinjer for leverandørstyring ift. informationssikkerhed i Plan- og Landdistriktsstyrelsen

1. Indledning

Retningslinjerne skal danne grundlaget for, at styrelsen kan fastholde et højt sikkerhedsniveau i forbindelse med outsourcing, herunder nyanskaffelse af it-systemer.
I forbindelse med enhver indgåelse af nye leverandøraftaler eller genforhandling af eksisterende, skal der tages stilling til indholdet af aftalen jf. følgende punkter:

1. Planlægning
2. Kravsstillelse
3. Leverandørvalg
4. Aftale
5. Styring
6. Afslutning.

Når aftalen er indgået kommer fokus særligt på punkt 5 om styring af leverandørforholdet, da et højt sikkerhedsniveau kræver en løbende og tæt kontakt med leverandøren.

2. Planlægning

2.1. Væsentlighedsbetragtning

Styrelsen anvender en række forskellige it-systemer ifm. styrelsens opgaveløsning. Nedenstående retningslinjer skal følges, såfremt der er tale om større systemer, som er væsentlige for styrelsens drift, eller såfremt systemet håndterer kritisk information, herunder persondata.

Vær opmærksom på, at der gælder særlige krav, såfremt systemet er vurderet samfundskritisk, samt hvis leverandør kommer fra et såkaldt tredjeland (dvs. uden for EU). Bolig- og Planstyrelsen har aktuelt ikke systemer, der er klassificeret som samfundskritiske.

2.2. Kortlæg forretningsproces og udarbejde risikovurdering

Inden beslutningen om at outsource et it-system træffes, skal styrelsen kortlægge, hvordan it-infrastrukturen er sammensat, hvordan datastrømmene løber, og hvordan de indbyrdes afhængigheder og grænseflader mellem styrelsens it-systemer ser ud.

Ud fra analysen af datastrøm mv. skal kommende systemejer (eller projektleder) beskrive risici forbundet med outsourcing af systemet med fokus på sikring af fortrolighed, integritet og tilgængelighed af styrelsens data, så dette kan indgå i det videre arbejde med at definere evt. krav vedr. informationssikkerhed (se bilag 1 vedr. mulige punkter i risikovurderingen).

2.3. Risikohåndteringsplan

Når systemejer (på baggrund af oplæg fra projektleder) har afdækket relevante risici ved den planlagte outsourcing, bør der udarbejdes en plan for, hvordan disse risici skal håndteres i leverandørforholdet.

3. Kravsstillelse

Styrelsen skal stille krav til leverandørens håndtering af cyber- og informationssikkerhed, der bidrager til at nedbringe risici til et acceptabelt niveau og sikrer et tilstrækkeligt sikkerhedsniveau forbundet med leverancen. Kravene til leverandørens sikkerhedsstyring bør ledsages af krav vedrørende kontrol og opfølgning, der understøtter leverandørens efterlevelse af sikkerhedskravene i aftaleperioden.

I udarbejdelsen af sikkerhedskravene vil styrelsen tage udgangspunkt i god praksis og internationale standarder for cyber- og informationssikkerhed såsom ISO/IEC 27001 og 27002, tekniske minimumskrav til statslige myndigheder og/eller tilsvarende.

Der kan derfor som minimum anvendes følgende formulering, når der skal formuleres krav vedr. informationssikkerhed ifm. nye leverandøraftaler.

Standardformulering vedr. informationssikkerhed
"Leverandøren skal med henblik på løbende sikring af informationssikkerhed i tilknytning til levering af ydelserne opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO27001 eller tilsvarende (national eller international) anerkendt standard, samt de til enhver tid gældende tekniske minimumskrav for statslige myndigheder, baseret på en risikostyringsproces og i overensstemmelse med angivne specifikke krav til Leverandørens ISMS. Leverandøren skal herunder løbende tilpasse sit ISMS, såfremt Leverandørens opdatering af sin risikovurdering medfører et behov herfor."
[Denne tekst kan suppleres med detaljerede sikkerhedskrav, som ønskes fra styrelsens side]

For systemer, som vurderes forretningskritiske for styrelsen, og hvor styrelsens drift derfor er afhængig af adgang til system og data, bør der desuden formuleres krav til:

- *Recovery Time Objective (RTO)* – dvs. hvor hurtigt skal systemet være op at køre igen efter nedbrud
- *Recovery Point Objective (RPO)* – dvs. hvor ofte leverandøren skal foretage backup og dermed det tidsrum, inden for hvilket data kan mistes (foretages backup hver time, kan styrelsen således maksimalt miste en times arbejde/data)

Yderligere eksempler på krav og opmærksomhedspunkter fremgår af bilag 2.
Ved formulering af krav skal systemejer (projektleder) samtidig have for øje, hvordan disse kan kontrolleres og dokumenteres (smart-princip).

4. Leverandørvalg

Valg af leverandør har betydning for kvaliteten og sikkerheden forbundet med leverancen. Det er derfor vigtigt, at styrelsen vælger leverandør ud fra relevante kriterier og på baggrund af en grundig vurdering af leverandørens samlede evne til at opfylde styrelsens sikkerhedskrav og øvrige krav til opgaveløsningen (se bilag 3 indeholdende eksempler på kriterier for leverandørvalg).

I forhold til sikkerhed bør styrelsen vurdere, om de sikkerhedsforanstaltninger, leverandøren forpligter sig til at levere, står i et rimeligt og realistisk forhold til prisen, og hvor forretningskritisk systemet er for styrelsen.

Hvis leverandøren overlader dele af opgaveløsningen til en underleverandør, kan der opstå nye cyber- og informationssikkerhedsrisici. Det er derfor vigtigt, at styrelsen har overblik over forsyningskæden og tager stilling til risici forbundet med leverandørens brug af underleverandører.

Vær yderligere opmærksom på, at ved valg af udenlandske leverandører, herunder særligt fra såkaldte tredjelande (dvs. uden for EU), kan der være særlige forhold, der påvirker cyber- og informationssikkerhed samt hensynet til beskyttelse af persondata, herunder lokal lovgivning, andre myndigheders adgang til styrelsens data, øget risiko for hacking mv.

5. Aftale

Når styrelsen har valgt en leverandør, skal der udarbejdes et aftalegrundlag mellem parterne. Aftalen skal indeholde en beskrivelse af parternes roller og ansvar i forhold til at styre cyber- og informationssikkerheden i aftaleperioden.

I aftalen skal det være klart formuleret for leverandøren, hvilke forventninger styrelsen har til dennes cyber- og informationssikkerhed. Sikkerhedskravene bør skrives ind i kontrakten, så de kan håndhæves på lige fod med andre krav i kontrakten.

Aftalen skal også beskrive, hvordan det i aftaleperioden sikres, at leverandøren lever op til de fastsatte sikkerhedskrav.

Bestemmelserne i aftalen skal blandt andet omfatte leverandørens forpligtelser i forhold til dokumentation og rapportering til styrelsen samt styrelsens ret til - enten selv eller ved hjælp af en tredjepart - at føre kontrol med leverandørens efterlevelse af kontrakten.

Aftalen skal forpligte leverandøren til at afsætte de fornødne ressourcer til rapportering og kontrol, herunder tid til mødeforberedelse, udarbejdelsen af dokumentation og opfølgning.

Det skal fremgå af kontrakten, at styrelsen skal godkende leverandørens anvendelse af underleverandører i forbindelse med leverancen, ligesom krav til leverandørens håndtering af cyber- og informationssikkerhed ligeledes gælder for de underleverandører, som leverandøren måtte benytte i forbindelse med leverancen.

Leverandøren skal desuden være forpligtet til at bistå styrelsen i forbindelse med gennemførelsen af kontrollen, herunder ved at give styrelsen den fornødne fysiske og logiske adgang til leverandørens eller underleverandørers lokaliteter, it-systemer og data samt ved at udlevere alt relevant dokumentation.

Aftalen skal give parterne mulighed for løbende at justere sikkerhedsniveauet i takt med, at risikobilledet ændrer sig, eksempelvis ved at styrelsen stiller supplerende sikkerhedskrav til leverandøren. Dog skal aftalen sikre, at styrelsen skal godkende eventuelle justeringer hos leverandøren og dermed i sidste ende fastsætte sikkerhedsniveauet forbundet med leverancen.

Der kan tages udgangspunkt i eller hentes inspiration fra de kontraktskabeloner, som er udarbejdet af Digitaliseringsstyrelsen, når aftalen udarbejdes - se https://digst.dk/styring/standardkontrakter/.

5.1. Samarbejdsorganisation

Efter indgåelsen af kontrakten bør parternes driftsansvarlige afholde et opstartsmøde for at fastsætte de nærmere detaljer og drøfte eventuelle uklarheder i aftalen. Forventningsafstemningen kan bidrage til at sikre enighed om parternes respektive roller og forpligtelser samt forebygge misforståelser og tvister i aftaleperioden.

I aftalen bør indgå etablering af en samarbejdsorganisation og formaliseret proces for håndtering af dialogen mellem styrelsen og leverandør. Processen bør fastlægge den regelmæssige dialog mellem parterne, eskalationsveje til at løse eventuelle tvister og kommunikationsveje i tilfælde af, at der sker en sikkerhedshændelse eller opstår en beredskabssituation herunder udveksling af kontaktoplysninger på begge organisationers beredskabspersoner (se også styrelsens it-beredskabsplan).

Fra styrelsen vil systemejer og systemforvalter samt application manager være naturlige medlemmer af samarbejdsudvalget, evt. suppleret med andre daglige brugere af systemet (se bilag 4 vedr. rolle og ansvar ifm. leverandørstyring).

6. Styring

Der kan være stor forskel på, hvor ofte og udførligt styrelsen har behov for at føre kontrol med den enkelte leverandør. Omfanget og frekvensen af kontrollen bør derfor bero på en konkret vurdering af leverancens væsentlighed i forhold til styrelsens forretning og risici forbundet hermed. Denne vurdering bør dokumenteres og opdateres løbende afhængig af den konkrete leverance og eventuelle ændringer i risikobilledet.

Styrelsen bør altid styre leverandøren med udgangspunkt i kontrakten mellem parterne. Styrelsen kan f.eks. udvælge de sikkerhedskrav i kontrakten, som det er mest relevant at kontrollere leverandørens efterlevelse af på baggrund af en risikovurdering (se bilag 5 med forslag til værktøjer til styring af leverandør).

Hvis leverandøren ikke lever op til sikkerhedskravene, er det vigtigt, at styrelsen straks følger op på leverandørens afvigelser fra de aftalte krav og håndhæver kontrakten. Det er systemejers ansvar at påpege leverandørens manglende efterlevelse af kravene og kontrollere, at leverandøren efterfølgende træffer de fornødne sikkerhedsforanstaltninger og udbedrer eventuelle fejl eller mangler i overensstemmelse med kontrakten.

Styrelsen bør også sikre, at den gennemførte kontrol dokumenteres af hensyn til eventuel håndhævelse af kontrakten ved fx referat af møder omhandlende informationssikkerhed, opdatering af risikovurdering og udarbejdede handleplaner ved erkendt mangler i informationssikkerheden.

Samarbejdsorganisation jf. punkt 4 bør mødes regelmæssigt og som minimum en gang om året for at gennemgå status for samarbejdet og leverancen samt status for informationssikkerhed og de i aftalen oplistede sikkerhedskrav.

Risikovurderinger bør ligeledes opdateres minimum årligt samt ved væsentlige sikkerhedshændelser og væsentlige ændringer mhp. at vurdere, om sikkerhedsniveauet skal justeres som følge af ændringer i risikobilledet. Leverandøren kan her især bidrage til at identificere relevante risici og vurdere deres sandsynlighed og tekniske konsekvenser. Det skyldes, at leverandøren har større kendskab til egne sikkerhedsforanstaltninger og it-infrastrukturen, der understøtter leverancen. Styrelsen bør derfor sikre, at leverandøren bidrager med viden om relevante trusler og sårbarheder til styrelsens risikovurdering.

Parterne bør løbende vurdere, dokumentere og håndtere væsentlige ændringer i aftaleperioden som en del af deres styring af cyber- og informationssikkerhed. Styrelsen bør sikre, at leverandøren følger rettidigt op på eventuelle ændringer ved at foretage fornødne justeringer og træffe supplerende sikkerhedsforanstaltninger i henhold til aftalen. Der kan blandt andet ske ændringer i parternes organisation, forretningsprocesser og it-infrastruktur i aftaleperioden. Styrelsen bør være særlig opmærksom på forhold hos leverandøren, der kan påvirke sikkerheden i leverancen, såsom ændringer i leverandørens forretningsstrategi, økonomiske forhold og brug af underleverandører.

I forhold til omgivelserne bør styrelsen især være opmærksom på den teknologiske udvikling, forandringer i trusselsbilledet og ændringer i den regulering, som parterne er underlagt.

Derudover bør styrelsen sikre, at leverandøren håndterer eventuelle sikkerhedshændelser i aftaleperioden i overensstemmelse med kontrakt.

Det er leverandørens ansvar at føre kontrol og tilsyn med de delleverancer, som underleverandøren leverer til styrelsen, herunder inddrager underleverandør i det løbende arbejde med opdatering af risikovurderinger. Styrelsen skal i dialogen med leverandøren tilse, at denne kontrol gennemføres og dokumenteres.

6.1. Særligt vedr. Statens IT (SIT)

For de statslige myndigheder, hvor ansvaret for organisationens it og driften heraf er ressortoverdraget til SIT, er tilsynet med SIT overgået til Finansministeriet (FM).

FM's departement fører derfor blandt andet tilsyn med SIT's styring af cyber- og informationssikkerheden og deler resultaterne heraf med SIT's kunder. Dét fritager som udgangspunkt styrelsen for selv at føre tilsyn med SIT. I stedet skal styrelsen forholde sig til, om FM's løbende tilsynsrapporter og årlige tilsynsberetning fremhæver relevante risici eller indeholder bemærkninger til sikkerhedsniveauet hos SIT, der har betydning for sikkerheden forbundet med de outsourcede it-systemer til SIT.

Resultatet af FM's analyser skal derfor præsenteres for informationssikkerhedsudvalget på førstkommende møde.

Ved outsourcing til SIT bør styrelsen dog stadigvæk foretage en risikovurdering af det pågældende it-system. På baggrund heraf bør styrelsen vurdere, om sikkerheds-

foranstaltningerne beskrevet i SIT's såkaldte varedeklaration tilsammen sikrer et tilstrækkeligt sikkerhedsniveau, eller om der er behov for yderligere sikkerhedsforanstaltninger.

Afhængig af den af styrelsen valgte driftsmodel kan der være dele af teknologistakken, som ikke er omfattet af FM's tilsyn, herunder hvis styrelsens risikovurdering fører til yderligere sikkerhedskrav. I så fald vil denne tilsynsopgave påhvile styrelsen og ikke FM.

Da FM har overtaget tilsynsopgaven, bør styrelsen orientere FM's departement, hvis SIT's risikohåndtering vurderes at være utilstrækkelig, eller der i aftaleperioden opstår tvister mellem SIT og styrelsen om konkrete forhold i kontrakten.

7. Afslutning

Når aftalen ophører, bør niveaet for styrelsens cyber- og informationssikkerhed opretholdes under afviklingen af leverandørforholdet. Dette gælder uanset om driften overdrages til en anden leverandør, eller om styrelsen vælger at overtage driftsopgaven (insourcing).

Styrelsen og leverandøren bør udarbejde en plan for, hvordan det aftalte sikkerhedsniveau opretholdes under hele afviklingsforløbet. Planen bør beskrive de sikkerhedsforanstaltninger, der skal være til stede hos parterne, hvis driften føres tilbage til styrelsen eller overdrages til en ny leverandør.

Ved ophøret af samarbejdet med leverandøren bør styrelsen også sørge for rettidigt at fjerne alle leverandørens fysiske og logiske adgangsrettigheder til styrelsens aktiver, herunder styrelsens informationer, it-systemer og lokaliteter. Af kontrakten bør det fremgå, hvilke aktiver der skal leveres tilbage til styrelsen, bortskaffes eller overdrages til en ny leverandør. Aftalen bør ligeledes beskrive procedurer til at sikre leverandørens forsvarlige overdragelse og bortskaffelse af styrelsens aktiver med hensyn til format, fuldstændighed, dokumentation, verificering, sikkerhed med mere.

Parterne kan desuden aftale, at leverandøren fortsat opbevarer visse informationer for styrelsen i en periode efter samarbejdets formelle ophør. Leverandøren kan eksempelvis opbevare logfiler indsamlet i aftaleperioden, så det fortsat er muligt at foretage undersøgelser af potentielle it-sikkerhedshændelser hos leverandøren.

8. Referencer

https://sikkerdigital.dk/myndighed/iso-27001-implementering/leverandoerstyring
https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/Vejledning-cybersikkerhed-i-leverandorforhold_cfsc_digst-2022.pdf

Version	*1*
Ændring siden sidste version	
Dato	1. august 2024
Godkendt af	Underdirektøren

Bilag 1 - Kriterier for risikovurdering af outsourcing af IT
Herunder er beskrevet kriterier, som kan indgå i en risikovurdering af outscourcing af it-systemer – listen er ikke udtømmende, hvorfor systemejer (projektleder) kan lade yderligere punkter indgå i vurderingen.

- Væsentlige forandringer hos leverandøren, der kan påvirke leverancen. Leverandøren kan eksempelvis flytte til et andet land, gå konkurs, skifte underleverandør eller blive opkøbt af en anden virksomhed.

- Ved outsourcing overlades dele af styrelsen risikohåndtering til leverandøren. Styrelsen bør derfor sikre, at leverandøren løbende bidrager til risikovurdering, eksempelvis med særlig viden om relevante trusler og sårbarheder.

- Der kan være uoverensstemmelse mellem styrelsens sikkerhedsbehov og leverandørens risikoappetit og sikkerhedsniveau, hvilket kan føre til utilstrækkelig risikohåndtering. Omvendt kan outsourcing potentielt forbedre styrelsens sikkerhed afhængig af niveauet af leverandørens håndtering af cyber- og informationssikkerhed.

- Cybertruslen fra cyberkriminalitet og cybespionage, da outsourcing kan øge styrelsens angrebsflade for hackere. Der er blandt andet risiko for supply chain-angreb, hvor hackere forsøger at kompromittere styrelsen ved at udnytte sårbarheder hos leverandøren eller leverandørens andre kunder.

- Medarbejdere hos leverandøren og eventuelle underleverandører, som styrelsen ikke har ledelsesretten over, kan få fysisk og logisk adgang til styrelsens aktiver.

- Leverandøren kan få kendskab til styrelsens organisation, forretningsprocesser, it-infrastruktur, sikkerhedsforanstaltninger, interne procedurer m.m.

- Leverandørens villighed til at levere den efterspurgte dokumentation, og styrelsens mulighed for at føre kontrol med leverandøren kan være begrænset.

- Eventuelle lovkrav og anden regulering på området, der kan medføre risici for styrelsen ved manglende efterlevelse heraf hos kunden eller leverandøren.

Bilag 2 - Eksempler på leverandørkrav ifm. informationssikkerhed

Forhold vedrørende cyber- og informationssikkerhed	Forhold vedrørende leverandørstyring
• Relevante lov- og myndighedskrav, herunder de tekniske minimumskrav, katalog over kontraktbestemmelser for samfundskritiske it-systemer, lokationskravet, sikkerhedscirkulæret og databeskyttelsesreglerne. • Leverandørens risikostyringsproces og opretholdelse af et ledelsessystem for informationssikkerhed baseret på ISO 27001 eller tilsvarende. • Rolle- og ansvarsfordelingen mellem styrelse og leverandør (se afsnit 4). • Behovet for at indgå en databehandleraftale med leverandøren. • Uddannelse og træning af relevante medarbejdere hos leverandøren og evt. underleverandører med adgang til styrelsens aktiver. • Behovet for sikkerhedsgodkendelse af relevante medarbejdere hos leverandøren og evt. underleverandører med adgang til styrelsens aktiver. • Parternes gensidige tavshedspligt, der også omfatter underleverandører. • Parternes håndtering af cyber- og informationssikkerhed i overgangsperioden fra en evt. tidligere leverandør.	• Leverandørens rapportering, herunder rapporteringens form og indhold samt struktur og frekvens for statusmøder mellem parterne. • Styrelsens ret til at føre kontrol med leverandørens efterlevelse af kontrakten og gældende regulering på området (compliance). • Leverandørens brug af underleverandører. • Leverandørens forpligtelse til at udpege relevante nøglepersoner i organisationen, der er centrale ift. leverandørens opfyldelse af kontrakten. • Leverandørens etablering af en samarbejdsorganisation (se afsnit 4). • Leverandørens forpligtelse til at samarbejde med styrelsens øvrige leverandører. • Styrelsens mulighed for at inddrage tredjeparter til støtte ifm. leverancen og ved aftalens ophør (f.eks. teknisk eller juridisk bistand). • Leverandørens forpligtelse til at levere retvisende, fyldestgørende og til enhver tid ajourført dokumentation for udførelsen af leverancen. • Parternes proces for håndtering af ændringer ift. løbende at til-

• Gennemførelse af sikkerhedstests og sårbarhedsscanninger (af styrelsen, leverandøren eller en tredjepart). • Leverandørens adgangsstyring ift. adgangen til styrelsens aktiver, herunder at leverandøren skal understøtte styrelsens klassifikationssystem. • Parternes procedurer for hændelseshåndtering, forretningsvidereførelse og beredskab, herunder regelmæssig test af beredskabsplaner. • Leverandørens underretningspligt over for styrelsen om forhold, der kan påvirke sikkerheden forbundet med leverancen, herunder sikkerhedshændelser. • • Sikker kommunikation mellem parterne, herunder f.eks. brug af TLS og DMARC. For flere anbefalinger herom se CFCS' vejledninger på cfcs.dk.	passe cyber- og informationssikkerheden i aftaleperioden (se afsnit 4). • Bestemmelser, der tager højde for et evt. salg, ændring i ejerforhold eller ophør af leverandørens virksomhed. • Bestemmelser vedrørende leverandørens forpligtelse til at afhjælpe fejl og mangler i leverancen. • Leverandørens forpligtelser til rettidigt at træffe supplerende eller udbedrende sikkerhedsforanstaltninger ved misligholdelse af sikkerhedskrav. • Procedurer for håndtering af tvister. • Konsekvenser ved leverandørens misligholdelse af sikkerhedskrav, der bør kunne medføre bod og give styrelsen ret til straks at ophæve kontrakten. • • Ophørsbestemmelser ved afvikling af styrelse-leverandørforholdet (se afsnit 6).

Du kan søge yderligere inspiration til udarbejdelsen af sikkerhedskrav i materialet på Digitaliseringsstyrelsens hjemmeside (digst.dk). Her findes bl.a. en række værktøjer og skabeloner, der kan hjælpe med at stille relevante sikkerhedskrav i kontrakter, herunder K04-standardkontrakt for it-drift, et klausulbibliotek og et kravkatalog.

Digitaliseringsstyrelsen (2016). Klausuler til informationssikkerhed. https://digst.dk/Styring/Standardkontrakter/Klausuler-til-informationssikkerhed

Digitaliseringsstyrelsen (2017). Sådan stiller du krav til leverandører om informationssikkerhed – katalog. https://digst.dk/styring/standardkontrakter/klausuler-til-informationssikkerhed/kravkatalog-til-leverandoerer/

Digitaliseringsstyrelsen (2020b). K04 Standardkontrakt for it-drift. https://digst.dk/styring/standardkontrakter/k04-standardkontrakt-for-it-drift/

Bilag 3 - Valg af leverandør

Nedenstående liste giver et overblik over relevante forhold, som styrelsen kan medtage i sin vurdering af potentielle leverandører i forbindelse med leverandørvalget:

- Leverandørens evne til at levere den ønskede ydelse, herunder størrelse og sandsynlighed for misligholdelse, konkurs mv.
- Leverandørens evne til at leve op til de stillede sikkerhedskrav.
- Leverandørens geografiske placering.
- Leverandørens accept af eventuelle overgangsforhold, hvis opgaven tidligere har været outsourcet til en anden leverandør.
- Leverandørens villighed til at samarbejde og til at lade sig efterse/revidere.
- Leverandørens accept af ophørsbestemmelser, herunder forpligtelsen til at opretholde cyber- og informationssikkerheden i hele ophørsperioden (se afsnit 6).
- Leverandørens økonomiske forhold og ejerforhold.
- Leverandørens brug af underleverandører.
- Leverandørens integritet og eventuelle konstaterede tilfælde af væsentlig misligholdelse af tidligere offentlige kontrakter.
- Størrelses- og afhængighedsforholdet mellem styrelse og leverandør.
- Risikoen for leverandørlåsning pga. omkostningerne ved senere at skifte leverandør, når styrelsen først er blevet afhængig af leverandørens ydelser.

Bilag 4 – roller og ansvar ifm. leverandørstyring (se også styrelsens it-governancemodel)

Roller	Opgaver og ansvar
Ledelsen	• Overordnet ansvarlig for organisationens styring af cyber- og informationssikkerhed, herunder den interne organisering, etablering af et ledelsessystem (ISMS) og fastsættelse af organisationens sikkerhedsniveau. • Ansvarlig for de strategiske beslutninger vedrørende outsourcing. • Skal godkende relevante styringsdokumenter såsom en politik for organisationens styring af cyber- og informationssikkerhed ved outsourcing. • Skal sikre, at organisationen har de fornødne ressourcer og kompetencer til leverandørstyring og styring af cyber- og informationssikkerhed. • Skal vurdere organisationens behov for ekstern rådgivning og bistand ved udarbejdelsen af kontrakten og den efterfølgende leverandørstyring. • Skal godkende risikovurderinger og risikohåndteringsplaner
Informationssikkerhedskoordinator / it-sikkerhedsansvarlig	• Daglig ansvarlig for organisationens styring af cyber- og informationssikkerhed, herunder den tværgående koordination og kommunikation. • Skal sikre sammenhæng mellem sikkerhedskravene i kontrakten og organisationens politikker, procedurer og retningslinjer for cyber- og informationssikkerhed. • Skal sikre, at der føres tilstrækkelig kontrol med leverandørens efterlevelse af sikkerhedskravene i kontrakten. • Skal sikre, at der løbende gennemføres risikovurderinger og udarbejdes risikohåndteringsplaner i forbindelse med outsourcing.
Kontraktansvarlig	• Ansvarlig for den generelle styring og håndhævelse af kontrakten. • Skal sikre, at kontrakten opdateres ved ændringer i aftalegrundlaget. • Skal sikre, at leverandøren udbedrer evt. fejl og mangler i leverancen.

	• Skal håndtere evt. tvister med leverandøren og eskalere til ledelsen efter behov.
Jura	• Ansvarlig for organisationens efterlevelse af de udbudsretlige regler og overholdelse af andre relevante lov- og myndighedskrav ved outsourcing. • Skal bistå med juridisk rådgivning i forbindelse med outsourcing, herunder juridisk kvalitetssikring af sikkerhedskrav og kontrakten som helhed
System- og dataejere Støttet af systemforvalter	• Ansvarlig for cyber- og informationssikkerheden forbundet med it-systemer og data ved outsourcing, herunder leverandørstyring. • Skal klassificere it-systemer og data omfattet af kontrakten. • Skal identificere relevante sikkerhedskrav i kontrakten med udgangspunkt i organisationens sikkerhedsniveau og klassifikationssystem. • Skal kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten og følge op på eventuelle sikkerhedshændelser hos leverandøren. • Skal styre leverandørens adgang til organisationens it-systemer og data. • Skal gennemføre risikovurderinger i forbindelse med outsourcing og udarbejde risikohåndteringsplaner
Application manager	• Skal bistå med teknisk rådgivning i forbindelse med outsourcing, herunder hjælp til at identificere relevante sikkerhedskrav i kontrakten.
Databeskyttelsesrådgiver (DPO)	• Skal bistå med teknisk rådgivning i forbindelse med outsourcing, herunder hjælp til at identificere relevante sikkerhedskrav i kontrakten. • Skal kontrollere organisationens efterlevelse af databeskyttelsesreglerne. • Skal bistå med rådgivning ved indgåelse af en databehandleraftale med leverandøren og overvåge overholdelsen heraf i kontraktperioden

Bilag 5 - Eksempler på kontrol og opfølgning hos leverandøren

Styrelsens kontrol med leverandøren kan foregå på forskellige måder og omfatte flere former for dokumentation og rapportering. Leverandørens dokumentation kan blandt andet bestå af følgende:

- Skriftlige rapporter
- Erklæringer
- Risikovurderinger
- Styringsdokumenter

Derudover kan kontrollen omfatte en række aktiviteter såsom:

- Statusmøder mellem styrelse og leverandør (faste møder eller ad hoc).
- Skriftlig rapportering til styrelsen (fast afrapportering eller ved anmodning).
- Tilsyn hos leverandøren (enten varslet eller uanmeldt besøg).
- Intern audit/gennemgang eller egenkontrol foretaget af leverandøren.
- Ekstern audit/gennemgang foretaget af styrelsen eller en uvildig tredjepart.
- It-revision foretaget af certificerede revisorer.
- Beredskabsøvelser med styrelsen som deltager eller observatør.
- Sikkerhedstekniske undersøgelser (også kaldet penetrationstests).

Bilag 6 – ophørsbestemmelser ved afslutning af kontrakt.
Ved indgåelsen af aftalen med leverandøren bør styrelsen sikre sig, at ophørsbestemmelserne i aftalen som minimum omfatter følgende forhold:

- Leverandørens forpligtelser og fortsatte servicemål i ophørsperioden, hvis aftalen frivilligt opsiges eller ophører som følge af tvister mellem parterne.

- Styrelsens krav til cyber- og informationssikkerhed i styrelse-leverandørforholdet, mens opgaven overdrages til en anden leverandør eller overtages af styrelsen.

- En komplet liste over styrelsens aktiver (inklusiv backup) opbevaret hos leverandøren, der skal leveres tilbage til styrelsen, overdrages til en ny leverandør eller bortskaffes.

- Procedurer, der sikrer, at styrelsens aktiver leveres tilbage til styrelsen, overdrages til en anden leverandør eller bortskaffes, som beskrevet i aftalen.

- Parternes fortsatte tavshedspligt efter aftalens ophør.

- Leverandørens forpligtelse til at bidrage til en smidig overgang og videreførelse af driften, hvis opgaven skal i genudbud, overdrages til en ny leverandør eller hjemtages af styrelsen, herunder krav til leverandørens udlevering af dokumentation, overførsel af viden og samarbejde i overgangsperioden.