

VA-01

Bilag 1 – Kundens behovsbeskrivelse og kravspesifikasjon

Nytt fagsystem

GARANTIKASSEN FOR FISKERE

1	Avtalens punkt 1.1 Avtalens omfang.....	4
2	Avtalens punkt 2.4.1 Omfanget av vedlikeholdstjenesten	5
2.1	Applikasjonsdrift.....	5
2.1.1	Driftsovervåkning	6
2.1.2	Hendelseshåndtering.....	7
2.1.3	Logg- og sporbarhetsforvaltning	7
2.1.4	Databasetjenester	8
2.1.5	Integrasjonsdrift	8
2.1.6	Sikkerhetsrelaterte driftsoppgaver.....	9
2.1.7	Kapasitetsstyring	9
2.1.8	Beredskap.....	9
2.2	Korrigerende vedlikehold	10
2.3	Adaptivt vedlikehold.....	11
2.4	Perfektivt vedlikehold.....	12
2.5	Preventivt vedlikehold.....	12
2.6	Regelverksforvaltning	13
2.7	Videreutvikling.....	14
2.8	Test og kvalitetssikring	14
2.9	Håndtering av produksjonsendring, release og produksjonssetting	15
2.10	Tilbakeføring og gjenoppretting	16
2.11	Konfigurasjonsstyring	16
2.12	Sikkerhet	17
2.13	Kompetanseoverføring	18
2.14	Rapportering.....	18
3	Avtalens punkt 2.4.3 – Oppdatering av dokumentasjon	19
4	Avtalens punkt 7.1 – Eksterne rettslige krav og tiltak generelt.....	20
4.1	Generelle krav	21
4.2	Ansvarsavgrensning.....	21
5	Avtalens punkt 7.2 – Informasjonssikkerhet.....	22
5.1	Risikostyring.....	22
5.2	Tilgangsstyring	22
5.3	Beskyttelse av data	23

5.4	Logging og sporbarhet	23
5.5	Sårbarhetshåndtering.....	23
5.6	Sikkerhetshendelser	24
5.7	Utvikling og endringer	24
5.8	Kontinuitet og gjenoppretting	24
5.9	Proaktiv sikkerhetsplikt	24
5.10	Forvaltning av tredjepartsrisiko.....	25
5.11	Sertifiseringer og sikkerhetsrevisjoner	25
5.12	Kontinuitetskrav	26
6	Exit, reversibilitetskrav og leverandørskifte	27
6.1	Formål og prinsipper	27
6.2	Exit-plan	27
6.3	Data og dokumentasjon	28
6.4	Kildekode og øvrige leveranseobjekter	28
6.5	Kompetanseoverføring og bistand ved leverandørskifte	28
6.6	Samarbeidsplikt	29
6.7	Testing av exit-plan.....	29
7	Tredjepartsavhengigheter	30

1 Avtalens punkt 1.1 Avtalens omfang

Dette bilaget beskriver Kundens krav til vedlikeholds-, forvaltnings- og videreutviklingstjenester for løsningen etablert gjennom anskaffelsen «Nytt fagsystem».

Bilaget utfyller SSA-V og angir krav til omfang, innhold, kvalitetsnivå, ansvarsområder og leveranser som skal inngå i avtalen.

Formålet med avtalen er å sikre stabil, sikker og kostnadseffektiv forvaltning av løsningen gjennom hele avtaleperioden, samt å legge til rette for kontinuerlig forbedring og videreutvikling.

Avtalen skal også sikre at løsningen forvaltes slik at den til enhver tid understøtter Kundens virksomhetsprosesser, regelverk og brukerbehov på en måte som muliggjør fremtidig leverandørskifte, og slik at virksomhetsregler, ordningsregler og parameterstyrte forhold i størst mulig grad kan endres uten behov for programkodeendringer og uten unødig risiko for eksisterende funksjonalitet.

Avtalen omfatter forvaltning, vedlikehold og videreutvikling av hele den etablerte løsningen, detaljert i Bilag 3 (VA-03), og nye elementer som tilkommer løsningen i vedlikeholdsperioden.

2 Avtalens punkt 2.4.1 Omfanget av vedlikeholdstjenesten

Leverandøren skal levere tjenester som beskrevet nedenfor.

Ved avtalens ikrafttredelse skal Leverandøren etablere vedlikeholds- og forvaltningstjenestene slik at disse kan leveres i samsvar med avtalens krav fra avtalt oppstartstidspunkt.

Etableringen skal omfatte de aktiviteter som er nødvendige for å sette tjenestene i operativ drift, herunder etablering av styrings- og rapporteringsrutiner, kontaktpunkter, beredskap, overvåkning og øvrige prosesser som følger av avtalen.

Etableringen skal være gjennomført før ordinær tjenesteleveranse etter avtalen påbegynnes.

2.1 Applikasjonsdrift

Applikasjonsdrift omfatter alle aktiviteter som er nødvendige for å sikre stabil, sikker og effektiv drift av Kundens fagsystem og dets tilhørende komponenter, uavhengig av hvem som leverer den underliggende infrastrukturen.

Formålet med applikasjonsdrift er å sikre at løsningen til enhver tid:

- er tilgjengelig i henhold til avtalte tjenestenivåer
- fungerer i samsvar med spesifiserte krav
- opprettholder avtalt sikkerhetsnivå
- opprettholder avtalt ytelse
- understøtter virksomhetskritiske prosesser
- ivaretar krav til sporbarhet og revisjon

Applikasjonsdrift omfatter drift av:

- applikasjoner/moduler
- tjenester
- regelmotor
- dokumentproduksjon
- integrasjoner
- databaser på applikasjonsnivå

- batchjobber og andre planlagte automatiserte jobber/prosesser
- overvåkningskomponenter

Overvåkning, hendelseshåndtering og logg- og sporbarhetsforvaltning skal samlet gi tilstrekkelig driftsinnsikt og sporbarhet til å muliggjøre proaktiv drift, effektiv feilsøking og rask identifisering og håndtering av avvik og hendelser.

2.1.1 Driftsovervåkning

Formålet med driftsovervåkning er å gi løpende innsikt i løsningens tilstand, ytelse og virksomhetskritiske prosesser.

Leverandøren skal etablere og opprettholde proaktiv driftsovervåkning som gir løpende innsikt i løsningens tilgjengelighet, ytelse, ressursutnyttelse, integrasjoner og virksomhetskritiske prosesser. Overvåkningen skal baseres på relevante måledata og visualiseringer og gjøre det mulig å identifisere avvik og uønskede utviklingstrekk på et tidlig tidspunkt.

Leverandøren skal etablere måledata og dashbord for blant annet:

- tilgjengelighet
- responstider og behandlingstider
- teknisk ressursforbruk og kapasitetsutnyttelse
- transaksjonsvolumer
- feilrater og feilmengder
- integrasjonsstatus og meldingsflyt
- gjennomføring av batchjobber og øvrige planlagte automatiserte jobber/prosesser
- status for virksomhetskritiske prosesser

Avvik, feil og unormale forløp i virksomhetskritiske prosesser skal automatisk kunne identifiseres og varsles, og deretter følges opp gjennom etablerte prosesser for hendelseshåndtering.

Kunden skal ha lesetilgang til relevante dashbord og rapporter som er nødvendige for å følge opp tjenestens tilgjengelighet, ytelse, hendelser, integrasjoner og øvrige avtalte tjenestenivåer.

2.1.2 Hendelseshåndtering

Formålet med hendelseshåndteringen er å forstå avvikene og gjenopprette normal tjeneste.

Leverandøren skal etablere og opprettholde en strukturert hendelseshåndtering som benytter informasjon fra overvåkning, måledata, logger og sporingsinformasjon til raskt å identifisere, analysere og håndtere hendelser samt redusere risikoen for gjentakelse.

Leverandøren skal:

- analysere hendelser ved bruk av tilgjengelige måledata og sporingsinformasjon
- identifisere berørte komponenter, integrasjoner og virksomhetsprosesser
- identifisere årsakskjeder og konsekvenser
- dokumentere hendelsesforløp og læringspunkter
- etablere korrigerende og forebyggende tiltak

Hendelser kategoriseres etter alvorlighetsgrad, registreres og responderes på samme måte som feil.

Ved kritiske (kategori A) og alvorlige (kategori B) hendelser skal Kunden varsles uten ugrunnet opphold og holdes oppdatert til hendelsen er løst.

Leverandøren skal kunne redegjøre for:

- når hendelsen oppstod
- hvordan hendelsen utviklet seg
- hvilke komponenter og prosesser som ble berørt
- hvilke data som eventuelt ble påvirket
- hvilke tiltak som ble gjennomført
- hvordan tilsvarende hendelser kan forebygges

2.1.3 Logg- og sporbarhetsforvaltning

Leverandøren skal opprettholde logg- og sporbarhetsforvaltning som sikrer at hendelser, transaksjoner, dataendringer og brukeraktiviteter kan registreres, korreleres og spores på tvers av komponenter, integrasjoner og virksomhetskritiske prosesser.

Løsningen skal produsere tilstrekkelig sporingsinformasjon til at det er mulig å:

- følge transaksjonsforløp på tvers av tjenester og integrasjoner
- identifisere hvor feil og forsinkelser oppstår
- identifisere berørte data og prosesser

- analysere årsakskjeder og tidsforløp
- gjennomføre effektiv feilsøking og hendelseshåndtering

2.1.4 Databasetjenester

Leverandøren skal etablere og opprettholde databasetjenester på applikasjonsnivå som sikrer at løsningsens data forvaltes på en stabil, sikker og effektiv måte. Databasetjenestene skal bidra til å opprettholde avtalt tilgjengelighet, ytelse og datakvalitet, samt understøtte virksomhetskritiske prosesser, sporbarhet og revisjon.

For å sikre at løsningsens datagrunnlag til enhver tid er korrekt, konsistent og tilgjengelig skal tjenestene omfatte løpende:

- overvåkning og analyse av ytelse, kapasitetsutvikling, ressursutnyttelse, feil og øvrige forhold som kan påvirke løsningsens stabilitet og ytelse
- identifisering av behov for optimalisering
- bistand ved datakorrigeringer
- vedlikehold av datamodeller

Leverandørens har ikke ansvar for drift av databaseserveren som sådan.

2.1.5 Integrasjonsdrift

Leverandøren skal etablere og opprettholde integrasjonsdrift som sikrer stabil, sikker og effektiv utveksling av data og meldinger mellom løsningen og tilknyttede interne og eksterne systemer. Integrasjonsdriften skal bidra til å opprettholde avtalte tjenestenivåer, ivareta datakvalitet og sikre at virksomhetskritiske prosesser som er avhengige av integrasjoner fungerer som forutsatt.

Tjenesten skal:

- overvåke integrasjoner
- håndtere feil
- håndtere vesentlig redusert ytelse
- håndtere avviste meldinger
- følge opp avvik i integrasjoner som skyldes eksterne systemer eller tjenester, herunder dokumentere avviket, vurdere konsekvenser for løsningen, varsle Kunden ved behov og følge opp gjenoppretting av normal integrasjonsflyt innenfor Leverandørens ansvarsområde.

Det skal være mulig å spore transaksjonsforløp og meldingsflyt.

2.1.6 Sikkerhetsrelaterte driftsoppgaver

Leverandøren skal etablere og opprettholde sikkerhetsrelaterte driftsoppgaver som bidrar til å ivareta løsningsens konfidensialitet, integritet, tilgjengelighet og sporbarhet. Oppgavene skal sikre at sikkerhetsmekanismer, sikkerhetskongfigurasjoner og sikkerhetsrelaterte komponenter forvaltes og vedlikeholdes på en kontrollert og forsvarlig måte gjennom hele avtaleperioden.

Leverandøren skal:

- håndtere sertifikater, nøkler og hemmeligheter gjennom å ha oversikt, sikker oppbevaring, overvåkning for utløp, fornyelse, regelmessig og hendelsesutløst utskifting samt sperring eller tilbakekalling ved behov
- overvåke, varsle og følge opp sikkerhetshendelser
- installere sikkerhetsoppdateringer til løsninger levert av Leverandøren
- ivareta øvrige sikkerhetsrelaterte forhold som er nødvendig for å opprette avtalt og forsvarlig sikkerhetsnivå

2.1.7 Kapasitetsstyring

Leverandøren skal etablere og opprettholde kapasitetsstyring som sikrer at løsningen til enhver tid har tilstrekkelig kapasitet og ytelse til å understøtte avtalte tjenestenivåer og virksomhetskritiske prosesser.

Leverandøren skal løpende vurdere:

- vekst i volum
- belastningsmønstre
- datamengder
- responstider

Leverandøren skal varsle Kunden uten ugrunnet opphold dersom kapasitetsgrenser forventes nådd.

2.1.8 Beredskap

Leverandøren skal etablere og opprettholde en hensiktsmessig beredskap for å forebygge, håndtere og begrense konsekvensene av hendelser som kan påvirke løsningsens tilgjengelighet, sikkerhet, integritet eller virksomhetskritiske prosesser. Beredskapen skal sikre at kritiske hendelser identifiseres, eskaleres og håndteres raskt og koordinert, og at normal tjeneste kan gjenopprettes innen avtalte tjenestenivåer.

Beredskapen skal omfatte nødvendige prosedyrer, roller, ansvar og kommunikasjonsrutiner for håndtering av hendelser som kan medføre vesentlig påvirkning på løsningen eller Kundens virksomhet, herunder:

- produksjonsstans og alvorlige driftsforstyrrelser
- sikkerhetshendelser
- svikt i integrasjoner
- feil i utbetalingsprosesser

2.2 Korrigerende vedlikehold

Korrigerende vedlikehold omfatter analyse, feilsøking, feilretting, testing og produksjonssetting av tiltak som er nødvendige for å gjenopprette eller opprettholde avtalt funksjonalitet i løsningen.

Formålet med korrigerende vedlikehold er å rette feil som medfører at løsningen ikke fungerer i samsvar med avtalt funksjonalitet, dokumentasjon eller spesifiserte krav.

Som feil regnes enhver verifiserbar avvikstilstand der løsningen:

- produserer feil resultat
- ikke utfører avtalt funksjonalitet
- stanser eller oppfører seg uforutsigbart
- bryter avtalte sikkerhetskrav
- bryter avtalte integrasjonskontrakter
- bryter avtalte ytelses- eller tilgjengelighetskrav
- produserer feil eller mangelfull dokumentasjon, vedtak, rapportering eller utbetalingsgrunnlag

Korrigerende vedlikehold omfatter blant annet:

- feil i programkode
- feil i konfigurasjon
- feil i regelimplementasjon
- feil i integrasjoner
- feil i databaser eller datamodeller
- feil i dokumentproduksjon
- feil i autorisasjons- eller sikkerhetsmekanismer
- feil i arbeidsflyter og prosesslogikk
- feil som oppstår som følge av tidligere leverte endringer

Leverandøren skal:

- registrere og klassifisere feil i samarbeid med Kunden

- analysere årsak
- etablere midlertidige tiltak ved behov
- gjennomføre permanent feilretting
- teste rettelsen
- dokumentere årsak og løsning
- oppdatere relevant dokumentasjon

Midlertidige omgåelseløsninger (work arounds) anses ikke som permanent feilretting.

Dersom regelsettet eller konfigurasjonen endres som følge av nytt regelverk, nye satser, nye budsjetter eller nye faglige krav, skal dette ikke anses som korrigerende vedlikehold, men som regelverksforvaltning eller endringsoppdrag.

2.3 Adaptivt vedlikehold

Adaptivt vedlikehold omfatter endringer som er nødvendige for å opprettholde løsningens funksjonalitet som følge av endringer i omgivelsene løsningen opererer i.

Formålet er å sikre at løsningen fortsatt fungerer som forutsatt uten at det gjøres endringer i løsningens funksjonelle omfang.

Adaptivt vedlikehold omfatter blant annet:

- endringer som følge av nye versjoner av operativsystemer, databaser, plattformkomponenter eller rammeverk
- endringer som følge av nye versjoner av tredjepartsprodukter
- tilpasninger som følge av endringer i API-er eller integrasjonsgrensesnitt hos eksterne leverandører
- tilpasninger som følge av endringer i offentlige registre eller datakilder
- tilpasninger som følge av endringer i autentiserings- eller autorisasjonsløsninger
- tilpasninger som følge av nye tekniske sikkerhetskrav og sikkerhetsstandarder
- nødvendige tekniske tilpasninger ved endringer i Kundens infrastruktur eller driftsplattform

Leverandøren har et selvstendig og proaktivt ansvar for å identifisere og foreslå tiltak som er nødvendige for å opprettholde løsningens funksjonalitet, sikkerhet, kompatibilitet og etterlevelse av krav som følge av endringer i omgivelsene. Manglende bestilling fra Kunden fritar ikke Leverandøren fra plikten til å identifisere og fremme forslag til slike tiltak.

Dersom manglende gjennomføring av adaptive tiltak kan påvirke vedtak, beregninger, opptjening, premiegrunnlag, pensjoner, dagpenger, tilskuddsordninger, dokumentproduksjon, økonomiske oppgjør eller utbetalinger, skal Leverandøren varsle Kunden uten ugrunnet opphold og særskilt beskrive risikoen og anbefalt tidsfrist for gjennomføring av tiltakene.

2.4 Perfektivt vedlikehold

Perfektivt vedlikehold omfatter forbedringer av eksisterende funksjonalitet uten at løsningens overordnede funksjonelle omfang endres.

Formålet er å forbedre kvalitet, ytelse, brukervennlighet, robusthet, sikkerhet eller vedlikeholdbarhet.

Perfektivt vedlikehold omfatter blant annet:

- forbedring av responstider og ytelse
- optimalisering av databaser og integrasjoner
- forbedring av brukergrensesnitt og arbeidsflyt
- forbedring av feilmeldinger og brukerfeedback
- forbedring av overvåkning og logging
- forbedring av kodekvalitet og arkitektur
- reduksjon av teknisk gjeld
- forbedring av automatiserte tester og kvalitetskontroller
- forbedring av drifts- og forvaltningsprosesser
- forbedring av tilgjengelighet og universell utforming
- forbedring av sikkerhetsmekanismer utover rene feilrettinger

Leverandøren skal løpende overvåke og vurdere forhold som kan forbedre løsningens kvalitet, ytelse, brukervennlighet, sikkerhet, robusthet, vedlikeholdbarhet og kostnadseffektivitet. Dersom Leverandøren identifiserer forbedringsmuligheter, skal Kunden uten ugrunnet opphold informeres. Leverandøren skal samtidig fremlegge forslag til perfekte tiltak, herunder beskrivelse av forventet nytte, konsekvenser, risiko, avhengigheter, estimert ressursbehov og anbefalt prioritet.

Leverandøren skal minst én gang per år gjennomføre en helhetlig vurdering av løsningens tekniske tilstand og fremlegge en forbedringsplan som identifiserer teknisk gjeld, forbedringsområder og anbefalte perfekte tiltak for kommende periode.

2.5 Preventivt vedlikehold

Leverandøren skal aktivt overvåke forhold som kan påvirke løsningens evne til å ivareta sporbarhet, revisjonsevne, sikkerhet, regelmotor, dokumentproduksjon, integrasjoner og utbetalingsprosesser.

Dersom Leverandøren identifiserer forhold som kan medføre økt risiko for feilutbetalinger, sikkerhetsbrudd, datatap eller manglende etterlevelse av krav, skal Leverandøren uten ugrunnet opphold varsle Kunden og foreslå preventive tiltak, herunder beskrivelse av risiko, sannsynlige konsekvenser, anbefalte risikoreduserende tiltak, estimert ressursbehov, gjennomføringsplan og anbefalt prioritet

Preventivt vedlikehold omfatter blant annet:

- installasjon av sikkerhetsoppdateringer og sikkerhetsfikser
- utskifting eller oppdatering av komponenter som nærmer seg end-of-life
- lukking av identifiserte sårbarheter
- forbedring av overvåkning og alarmering
- forbedring av backup- og gjenopprettingsrutiner
- kapasitetsanalyser og forebyggende kapasitetsjusteringer
- gjennomgang av logger og driftsmønstre for å identifisere risikoområder
- gjennomgang av teknisk gjeld med sikte på å redusere fremtidig feilrisiko
- forebyggende tiltak som følge av revisjoner, sikkerhetsanalyser eller penetrasjonstester

2.6 Regelverksforvaltning

Leverandøren skal etablere og opprettholde regelverksforvaltning som sikrer at løsningen til enhver tid understøtter gjeldende lover, forskrifter, tariffbestemmelser, vedtekter og øvrige virksomhetsregler som er relevante for Kundens forvaltning av medlemskap, opptjening, pensjon, dagpenger, tilskuddsordninger, vedtak og økonomiske oppgjør.

Regelverksforvaltningen skal bidra til at endringer i regelverk og forretningsregler kan gjennomføres på en kontrollert, sporbar og effektiv måte, med minst mulig risiko for løsningens stabilitet og datakvalitet.

Leverandøren skal bistå Kunden med:

- etablering av nye regelsett
- analyse av regelendringer
- endring av regelsett
- versjonering av regelsett
- kvalitetssikring av regelkonfigurasjon
- test av regelendringer
- produksjonssetting av regelendringer etter godkjenning og avtale med Kunden.

Målet skal være at regelendringer i størst mulig grad kan gjennomføres uten programkodeendringer, og at regelimplementering til enhver tid er korrekt, konsistent og etterprøvbart.

2.7 Videreutvikling

Ref. avtalens pkt. 2.4.8

Leverandøren skal gjennom hele avtaleperioden kunne gjennomføre videreutvikling av løsningen innenfor etablert løsningsarkitektur og arkitekturprinsipper, domener og forvaltningsmodell uten vesentlig omstrukturering av løsningens grunnleggende komponenter.

Videreutvikling kan omfatte:

- nye fartøyordninger
- nye mannskapsordninger
- nye regelsett
- nye beregningsmodeller
- nye dokumenttyper
- nye rapporter
- nye API-er
- nye integrasjoner
- nye arbeidsprosesser
- utvidelser av saksbehandlerflater
- utvidelser av Min Side
- nye kontrollregler
- nye utbetalingsprosesser

Leverandøren skal kunne delta i analyse, design, utvikling, testing og produksjonssetting.

Forslag som bryter med etablerte prinsipper, skal særskilt begrunnes.

2.8 Test og kvalitetssikring

Leverandøren skal etablere og opprettholde testing og kvalitetssikring som sikrer at endringer, feilrettinger, konfigurasjonsendringer og nye versjoner av løsningen oppfyller avtalte funksjonelle og ikke-funksjonelle krav før produksjonssetting. Testing og kvalitetssikring skal bidra til å redusere risikoen for feil, driftsforstyrrelser og utilsiktede konsekvenser for virksomhetskritiske prosesser, samt sikre at løsningens kvalitet, stabilitet og sikkerhet opprettholdes gjennom hele avtaleperioden.

Testing og kvalitetssikring skal være risikobasert og stå i forhold til endringenes omfang, kompleksitet og kritikalitet. Leverandøren skal etablere hensiktsmessige rutiner for både statisk og dynamisk testing og kvalitetssikring, herunder gjennomgang av krav, design, kildekode og konfigurasjon, samt funksjonell testing, regresjonstesting, integrasjonstesting, ytelsetesting og sikkerhetstesting der dette er relevant. Leverandøren skal dokumentere testresultater og uten ugrunnet opphold informere Kunden om identifiserte avvik, risikoer og anbefalte tiltak.

Testing skal som minimum omfatte:

- funksjonell verifikasjon
- verifikasjon av beregninger
- verifikasjon av vedtaksutfall
- verifikasjon av dokumentproduksjon
- verifikasjon av integrasjoner
- verifikasjon av sporbarhet og revisjon
- regresjonstesting

2.9 Håndtering av produksjonsendring, release og produksjonssetting

Leverandøren skal etablere og opprettholde en kontrollert og sporbar prosess for håndtering av produksjonsendringer, release og produksjonssetting. Prosessen skal sikre at endringer planlegges, vurderes, testes, godkjennes og gjennomføres på en måte som opprettholder løsningens stabilitet, sikkerhet og tilgjengelighet, og som minimerer risikoen for driftsforstyrrelser og utilsiktede konsekvenser for virksomhetskritiske prosesser

Leverandøren skal:

- planlegge produksjonsendringer og produksjonssettinger
- etablere tilbakeføringsplaner
- teste og verifisere produksjonsendringer forut for produksjonssetting
- gjennomføre produksjonsendringer og produksjonssettinger etter forutgående godkjenning og avtale med Kunden
- gjennomføre etterkontroll av produksjonsendringer og produksjonssettinger
- dokumentere produksjonsendringer, releaseinnhold og produksjonssettinger

Produksjonsendringer og produksjonssetting skal kunne gjennomføres uten unødig nedetid, fortrinnsvis i avtalte vedlikeholdsvinduer

2.10 Tilbakeføring og gjenoppretting

Leverandøren skal etablere og opprettholde prosedyrer for tilbakeføring og gjenoppretting som sikrer at feil, uønskede konsekvenser eller driftsforstyrrelser som oppstår i forbindelse med endringer, feilrettinger, konfigurasjonsendringer, produksjonssettinger eller sikkerhetshendelser kan håndteres på en rask, kontrollert og sporbar måte.

Prosedylene skal bidra til å begrense konsekvensene av hendelser, gjenopprette normal tjeneste innen avtalte tjenestenivåer og sikre at løsningens data, funksjonalitet, sikkerhet og integritet ivaretas.

Leverandøren skal sikre at nødvendige tilbakeførings- og gjenopprettingstiltak er planlagt, dokumentert, testet og tilpasset endringenes omfang, kompleksitet og kritikalitet.

Gjennomførte tilbakeføringer og gjenopprettingstiltak skal dokumenteres og være fullt sporbare.

2.11 Konfigurasjonsstyring

Leverandøren skal etablere og opprettholde konfigurasjonsstyring som sikrer at løsningens konfigurasjoner forvaltes på en kontrollert, sikker og sporbar måte gjennom hele avtaleperioden. Konfigurasjonsstyringen skal bidra til å opprettholde løsningens stabilitet, integritet og vedlikeholdbarhet, samt sikre at konfigurasjonsendringer kan gjennomføres med minst mulig risiko for driftsforstyrrelser og utilsiktede konsekvenser for virksomhetskritiske prosesser.

Konfigurasjonsstyringen skal omfatte identifisering, registrering, versjonsstyring, endringshåndtering og dokumentasjon av alle vesentlige konfigurasjonselementer, herunder:

- systemkonfigurasjon
- regelkonfigurasjon
- sikkerhetskonfigurasjon
- integrasjonskonfigurasjon
- konfigurasjon av tekniske miljøer for henholdsvis utvikling, test, kvalitetssikring og produksjon

Alle endringer skal være sporbare og dokumenterte, og det skal til enhver tid være mulig å identifisere:

- gjeldende versjon
- tidspunkt for endring
- hvilke endringer som er gjennomført

- ansvarlig ressurs
- berørte komponenter
- hvilken produksjonsendring eller release og produksjonssetting endringen inngår i

Konfigurasjonsendringer skal kunne tilbakeføres på en kontrollert måte dersom dette er nødvendig.

2.12 Sikkerhet

Leverandøren skal sikre at løsningens sikkerhetsmekanismer til enhver tid understøtter kravene til identitetsarkitektur, soneinndeling, domeneautorisasjon, revisjonsspor, sporbarhet og behandling av person- og økonomidata. Sikkerhetstiltak skal utformes slik at de ikke svekker løsningens evne til å dokumentere grunnlaget for vedtak, beregninger, utbetalinger og kontrollhandlinger.

Formålet med sikkerhetsarbeidet er å sikre at løsningen til enhver tid oppfyller avtalte krav til:

- konfidensialitet
- integritet
- tilgjengelighet
- autentisitet
- sporbarhet
- etterprøvbarehet

Tjenesten omfatter:

- sikkerhetsoppdateringer
- patching
- sikkerhetsanalyser
- sikkerhetstesting
- sårbarhetshåndtering
- hendelseshåndtering
- oppfølging av sikkerhetsavvik

Dersom det identifiseres svakheter eller sikkerhetsbrudd som kan påvirke riktigheten av vedtak, beregninger, opptjening, premiegrunnlag, pensjoner, dagpenger, tilskuddsordninger, dokumentproduksjon, økonomiske oppgjør eller utbetalinger, skal Leverandøren uten ugrunnet opphold bistå Kunden med å begrense konsekvensene, identifisere berørte data og prosesser, foreslå korrigerende og forebyggende tiltak og etablere en plan for permanent utbedring.

2.13 Kompetanseoverføring

Kompetanseoverføring omfatter planlagte aktiviteter som sikrer at Kunden opprettholder tilstrekkelig kunnskap om løsningens funksjonelle, tekniske og forvaltningsmessige forhold til å kunne ivareta rollen som systemeier og oppdragsgiver gjennom avtaleperioden.

Formålet med kompetanseoverføring er å:

- redusere leverandøravhengighet
- sikre effektiv samhandling mellom partene
- understøtte informerte beslutninger om videreutvikling
- sikre kontinuitet ved personellskifter
- legge til rette for eventuell fremtidig leverandørovertakelse

Kompetanseoverføring skal være en integrert del av Leverandørens løpende forvaltningsarbeid og ikke begrenses til avslutning av avtalen.

2.14 Rapportering

Rapportering skal være analysebasert og ikke begrenses til opplisting av aktiviteter. Leverandøren skal fremheve forhold som kan påvirke løsningens stabilitet, sikkerhet, vedlikeholdbarhet, etterlevelse, kostnadsbilde eller videreutviklingsevne, samt gi anbefalinger om nødvendige tiltak.

Som et minimum skal Leverandøren på månedlig basis rapportere:

- åpne feil
- lukkede feil
- sikkerhetshendelser
- tilgjengelighet
- ytelse
- pågående endringer
- gjennomførte endringer
- planlagte aktiviteter
- risiko og anbefalte tiltak

3 Avtalens punkt 2.4.3 – Oppdatering av dokumentasjon

Leverandøren skal gjennom hele avtaleperioden vedlikeholde og holde dokumentasjonen oppdatert, herunder

- overordnet løsningsarkitektur
- systemarkitektur og komponentoversikt
- integrasjonsoversikt
- dokumentasjon i kildekode repository
- API-spesifikasjoner
- datamodeller og datakatalog
- konfigurasjon og parameteroppsett
- regelsett og regelkonfigurasjon
- sikkerhetsarkitektur/sikkerhetsdokumentasjon
- autorisasjons- og tilgangsmodell
- drifts- release- og deployprosedyrer
- testdokumentasjon
- driftsdokumentasjon
- overvåknings- og alarmeringsoppsett
- oversikt over tredjepartsprogramvare lisenser og avhengigheter
- kjente tekniske begrensninger og teknisk gjeld

Dokumentasjonen skal holdes løpende oppdatert og være tilgjengelig for Kunden gjennom hele avtaleperioden.

4 Avtalens punkt 7.1 – Eksterne rettslige krav og tiltak generelt

Løsningen og tjenestene skal til enhver tid understøtte etterlevelse av gjeldende lover, forskrifter, offentlige krav, standarder og bindende myndighetspålegg som er relevante for Kundens virksomhet og leveransene under avtalen.

Leverandøren skal opprettholde nødvendig kompetanse og etablere hensiktsmessige prosesser for løpende å identifisere, vurdere og håndtere endringer i eksterne rettslige krav som kan påvirke løsningen, tjenestene eller Kundens virksomhetsprosesser.

Leverandøren har et selvstendig og proaktivt ansvar for å:

- overvåke endringer i relevante lover, forskrifter, standarder og myndighetskrav,
- identifisere forhold som kan påvirke løsningens funksjonalitet, sikkerhet, tilgjengelighet, sporbarhet, revisjonsevne eller etterlevelse av krav,
- varsle Kunden uten ugrunnet opphold om identifiserte endringer og deres konsekvenser,
- analysere behovet for tilpasninger av løsningen eller tjenestene, og
- fremlegge forslag til nødvendige tiltak.

Leverandøren skal som minimum beskrive:

- hvilke krav som er endret eller forventes endret,
- hvilke deler av løsningen, tjenestene eller virksomhetsprosessene som påvirkes,
- risiko ved manglende gjennomføring,
- alternative løsnings- og gjennomføringsalternativer,
- estimert ressursbehov,
- anbefalt gjennomføringstidspunkt,
- eventuelle konsekvenser for drift, sikkerhet, brukere og integrasjoner.

Leverandøren skal etter Kundens bestilling bistå med planlegging, utvikling, testing, dokumentasjon, produksjonssetting og øvrige tiltak som er nødvendige for å oppfylle de eksterne rettslige kravene.

4.1 Generelle krav

Eksterne rettslige krav omfatter blant annet, men er ikke begrenset til:

- Forvaltningsloven
- Offentleglova
- Arkivlova med tilhørende forskrifter
- Personopplysningsloven og Personvernforordningen (GDPR)
- eForvaltningsforskriften
- Regelverk for økonomistyring i staten
- Bokføringsregelverket i den utstrekning det er relevant
- Krav til informasjonssikkerhet, internkontroll, sporbarhet og revisjon

Leverandøren skal sikre at løsningen til enhver tid kan understøtte:

- sporbarhet og revisjon av vedtak og økonomiske transaksjoner
- historikk og etterprøvbarhet
- dokumentasjon av saksbehandling og beslutningsgrunnlag
- krav til oppbevaring og tilgjengeliggjøring av data og dokumenter
- krav til informasjonssikkerhet og behandling av personopplysninger

Leverandøren kan ikke legge til grunn at Kunden selv identifiserer endringer i eksterne rettslige krav.

Manglende bestilling fra Kunden fritar ikke Leverandøren fra plikten til å identifisere, vurdere og varsle om forhold som med rimelighet må antas å kunne påvirke løsningens funksjonalitet, sikkerhet, etterlevelse av krav eller evne til å understøtte Kundens virksomhetsprosesser.

4.2 Ansvarsavgrensning

Domene- og virksomhetsspesifikke krav er Kundens spesifikke ansvar og ligger utenfor Leverandørens ansvarsområde. Dette omfatter blant annet:

- lov om pensjonstrygd for fiskere (fiskerpensjonsloven)
- Forskrift om dagpenger for fiskere og fangstfolk under arbeidsløshet (A-trygdforskriften)
- forskrifter og regelverk knyttet til tilskuddsordningene som forvaltes av Kunden

- krav knyttet til medlemskap, opptjening, premiegrunnlag, pensjon, dagpenger og tilskuddsordninger
- krav fra Fiskeridirektoratet og andre domene- og virksomhetsspesifikke offentlige registre og datakilder som løsningen er avhengig av

5 Avtalens punkt 7.2 – Informasjonssikkerhet

Løsningen og tjenestene skal til enhver tid oppfylle krav til informasjonssikkerhet som er nødvendige for å sikre konfidensialitet, integritet, tilgjengelighet og sporbarhet for informasjon og tjenester som omfattes av avtalen.

Leverandøren skal etablere, vedlikeholde og etterleve et dokumentert og risikobasert styringssystem for informasjonssikkerhet som omfatter både utvikling, forvaltning, applikasjonsdrift og leveranse av tjenestene under avtalen.

Leverandøren skal gjennomføre tjenestene i samsvar med anerkjente prinsipper og standarder for informasjonssikkerhet og følge krav fastsatt av Kunden, gjeldende lovgivning og relevante offentlige standarder og veiledninger.

5.1 Risikostyring

Leverandøren skal:

- etablere og vedlikeholde nødvendige sikkerhetstiltak
- løpende identifisere og vurdere sikkerhetsrisikoer
- gjennomføre risikoreduserende tiltak etter godkjenning fra Kunden
- dokumentere identifiserte risikoer og gjennomførte tiltak
- varsle Kunden uten ugrunnet opphold om identifiserte forhold som kan medføre vesentlig risiko for løsningen eller tjenestene

5.2 Tilgangsstyring

Tilganger for interne og eksterne brukere administreres av Kunden, og skal sikre at:

- tilganger tildeles etter prinsippet om tjenstlig behov
- tilganger gis med lavest nødvendige privilegium
- privilegerte tilganger er særskilt kontrollert og dokumentert
- tilganger jevnlig gjennomgås og oppdateres
- tilganger fjernes uten ugrunnet opphold når behovet opphører

Leverandøren skal sikre at leverandørens tilganger forvaltes etter samme prinsipper.

5.3 Beskyttelse av data

Leverandøren skal etablere tiltak som sikrer:

- beskyttelse mot uautorisert innsyn, endring, sletting og tap av data
- kryptering av data under overføring
- hensiktsmessig beskyttelse av data under lagring
- sikker håndtering av nøkler, sertifikater og andre konfidensialiteter
- sikker behandling av sikkerhetskopier

Sensitive data og personopplysninger skal ikke benyttes i utviklings- eller testmiljøer med mindre dette er særskilt avtalt og tilstrekkelige sikkerhetstiltak er etablert.

5.4 Logging og sporbarhet

Leverandøren skal etablere logging og sporbarhet som gjør det mulig å:

- identifisere brukere og systemer som har utført handlinger
- identifisere tidspunkt og omfang av handlinger
- identifisere endringer i data og konfigurasjon
- identifisere sikkerhetshendelser og forsøk på uautorisert tilgang
- understøtte revisjon, feilsøking og hendelseshåndtering.

Sikkerhetslogger skal beskyttes mot uautorisert tilgang og manipulasjon.

5.5 Sårbarhetshåndtering

Leverandøren skal etablere prosesser for:

- identifisering og vurdering av sårbarheter
- løpende sikkerhetsoppdateringer og patchhåndtering
- vurdering av teknologisk foreldelse og end-of-life-komponenter
- håndtering av identifiserte sikkerhetsrisikoer

Kritiske sårbarheter skal håndteres uten ugrunnet opphold og prioriteres etter risiko og potensiell konsekvens.

5.6 Sikkerhetshendelser

Leverandøren skal:

- etablere prosesser for registrering og håndtering av sikkerhetshendelser
- uten ugrunnet opphold varsle Kunden om sikkerhetshendelser som kan påvirke løsningen, data eller tjenestene
- begrense konsekvensene av sikkerhetshendelser
- bistå Kunden med analyse gjenoppretting og korrigerende tiltak
- dokumentere årsak konsekvenser og gjennomførte tiltak

Ved sikkerhetshendelser som kan påvirke vedtak, beregninger, utbetalinger, dokumentproduksjon, sporbarhet eller behandling av personopplysninger, skal Leverandøren prioritere hendelsen som kritisk.

5.7 Utvikling og endringer

Leverandøren skal sikre at:

- sikkerhet inngår som en integrert del av utviklings- test- og endringsprosesser
- sikkerhetsmessige konsekvenser vurderes før produksjonssetting
- endringer ikke reduserer etablert sikkerhetsnivå
- nye komponenter og integrasjoner vurderes med hensyn til sikkerhetsrisiko

5.8 Kontinuitet og gjenoppretting

Leverandøren skal etablere og vedlikeholde prosedyrer for:

- sikkerhetskopiering
- gjenoppretting av data og tjenester
- håndtering av alvorlige drifts- og sikkerhetshendelser
- periodisk verifikasjon av gjenopprettingsevne

5.9 Proaktiv sikkerhetsplikt

Leverandøren har et selvstendig og proaktivt ansvar for å identifisere, vurdere og varsle om forhold som kan påvirke informasjonssikkerheten. Manglende bestilling fra Kunden fritar ikke Leverandøren fra plikten til å identifisere og fremme forslag til nødvendige sikkerhetstiltak.

Leverandøren skal løpende gjennomføre sikkerhetsovervåkning, risikovurderinger, varsling og rådgivning om informasjonssikkerhet. Dersom det identifiseres behov for sikkerhetstiltak som innebærer endringer i løsningen eller tjenestene, skal Leverandøren beskrive tiltakene og konsekvensene av disse og fremlegge forslag til gjennomføring for Kunden.

5.10 Forvaltning av tredjepartsrisiko

Leverandøren skal etablere rutiner for løpende identifisering og oppfølging av sikkerhetsmessige forhold knyttet til tredjepartsavhengigheter.

Leverandøren skal:

- overvåke kjente sårbarheter (CVE – Common Vulnerabilities and Exposures)
- overvåke supportstatus og livssyklus
- vurdere sikkerhetsmessige konsekvenser av nye sårbarheter
- varsle Kunden uten ugrunnet opphold ved vesentlige sikkerhetsrisikoer
- foreslå nødvendige risikoreduserende tiltak

Ved identifiserte kritiske sårbarheter skal Leverandøren uten ugrunnet opphold foreslå nødvendige tiltak for å opprettholde et forsvarlig sikkerhetsnivå, og gjennomføre disse etter godkjenning av Kunden.

5.11 Sertifiseringer og sikkerhetsrevisjoner

Leverandøren skal etablere, vedlikeholde og etterleve et dokumentert styringssystem for informasjonssikkerhet som er basert på anerkjente standarder og beste praksis for virksomhetskritiske IKT-løsninger.

Leverandøren skal som minimum:

- etterleve prinsippene i ISO/IEC 27001 for styringssystem for informasjonssikkerhet
- etterleve relevante deler av ISO/IEC 27002 for sikkerhetstiltak
- etablere og vedlikeholde sikkerhetsprosesser for utvikling, forvaltning og applikasjonsdrift
- gjennomføre regelmessige sikkerhetsrevisjoner og sårbarhetsvurderinger
- etablere rutiner for løpende håndtering av sårbarheter og sikkerhetsavvik

Dersom Leverandøren er sertifisert etter ISO/IEC 27001 eller tilsvarende standard, skal sertifiseringen opprettholdes gjennom hele avtaleperioden.

Dersom Leverandøren ikke er sertifisert, skal Leverandøren på Kundens forespørsel dokumentere hvordan kravene i ISO/IEC 27001 og øvrige relevante standarder etterleves.

Leverandøren skal uten ugrunnet opphold informere Kunden dersom:

- sertifisering bortfaller
- sertifisering suspenderes
- vesentlige avvik identifiseres ved revisjon
- sikkerhetsforhold oppstår som kan påvirke leveransen eller Kundens risikoeksponering

Leverandøren skal minst én gang per kalenderår gjennomføre:

- sikkerhetsrevisjon
- sårbarhetsskanning
- vurdering av tredjepartsavhengigheter
- vurdering av komponenters sikkerhetsstatus og supportstatus

Resultater og identifiserte risikoer skal dokumenteres og gjøres tilgjengelige for Kunden.

5.12 Kontinuitetskrav

Leverandøren skal etablere og opprettholde nødvendige tekniske og organisatoriske tiltak for å sikre at løsningen kan gjenopprettes etter alvorlige driftsavbrudd, sikkerhetshendelser og andre hendelser som medfører tap av tilgjengelighet eller data.

Løsningen skal understøtte definerte mål for gjenopprettingstid (Recovery Time Objective - RTO) og gjenopprettingspunkt (Recovery Point Objective -RPO).

Med gjenopprettingstid (RTO) menes den maksimalt akseptable tiden fra en alvorlig hendelse oppstår til berørt tjeneste er gjenopprettet og tilgjengelig for bruk.

Med gjenopprettingspunkt (RPO) menes det maksimalt akseptable tapet av data målt som tiden mellom siste tilgjengelige datakopi og tidspunktet for hendelsen.

Leverandøren skal etablere, dokumentere og vedlikeholde nødvendige prosedyrer, sikkerhetskopieringsmekanismer, redundansløsninger og gjenopprettingsrutiner for å oppfylle avtalte RTO- og RPO-krav.

Leverandøren skal minst én gang per kalenderår gjennomføre og dokumentere testing av gjenopprettingsprosedyrer, herunder verifisering av avtalte RTO- og RPO-verdier.

Resultatet av testene, identifiserte svakheter og planlagte forbedringstiltak skal gjøres tilgjengelig for Kunden.

6 Exit, reversibilitetskrav og leverandørskifte

6.1 Formål og prinsipper

Løsningen skal forvaltes og videreutvikles på en måte som muliggjør et fremtidig leverandørskifte uten unødig risiko for tap av data, funksjonalitet, sikkerhet, sporbarhet, dokumentasjon eller kompetanse.

Leverandøren skal gjennom hele avtaleperioden tilrettelegge for at Kunden til enhver tid kan overføre forvaltning, drift og videreutvikling av løsningen til Kunden selv eller til en ny leverandør. Leverandøren skal ikke etablere unødige tekniske, organisatoriske eller kommersielle bindinger som vanskeliggjør et fremtidig leverandørskifte.

Exit og leverandørskifte skal planlegges og gjennomføres på en måte som begrenser risikoen for driftsforstyrrelser og leverandørlåsing, og som sikrer at Kunden kan videreføre drift, forvaltning og videreutvikling av løsningen på en forsvarlig og kostnadseffektiv måte.

6.2 Exit-plan

Senest seks måneder etter avtaleinngåelse skal Leverandøren utarbeide en exit-plan for gjennomføring av et kontrollert leverandørskifte.

Exit-planen skal oppdateres minst én gang per år og ved vesentlige endringer i løsningen.

Planen skal som minimum beskrive:

- roller og ansvar
- aktiviteter og milepæler
- avhengigheter og risikoforhold
- kompetanseoverføring
- dokumentasjonsleveranser
- datauttrekk og dataoverføring
- overføring av kildekode
- overføring av konfigurasjon og regelsett
- overføring av integrasjoner
- verifikasjon og testing av overføringen

6.3 Data og dokumentasjon

Ved avtalens opphør skal Leverandøren uten ugrunnet opphold overlevere all dokumentasjon og alle data som Kunden har rettigheter til etter avtalen.

Overleveringen skal som minimum omfatte:

- dokumentasjon iht. avtalens pkt. 2.4.3
- oversikt over alle tredjepartsavhengigheter
- endringshistorikk
- oversikt over kjente feil og teknisk gjeld
- logger og revisjonsspor

Dokumentasjon og data skal overleveres i åpne, alminnelig anvendte og maskinlesbare formater.

6.4 Kildekode og øvrige leveranseobjekter

Leverandøren skal ved avtalens opphør overlevere alle leveranseobjekter som Kunden har rettigheter til etter avtalen, herunder:

- kildekode
- byggeskript
- deployskript
- databaseendringsskript
- konfigurasjonsfiler
- testskript
- automatiseringsskript

Leverandøren skal ikke tilbakeholde informasjon som er nødvendig for videre forvaltning og videreutvikling av løsningen.

6.5 Kompetanseoverføring og bistand ved leverandørskifte

Ved avtalens opphør skal Leverandøren bistå Kunden og eventuell ny leverandør med å gjennomføre et kontrollert leverandørskifte.

Bistanden skal som minimum omfatte:

- overføringsmøter
- gjennomgang av systemarkitektur og sentrale designvalg

- gjennomgang av drifts- og forvaltningsprosesser
- gjennomgang av integrasjoner og sikkerhetsmekanismer
- bistand ved migrering av integrasjoner
- gjennomgang av regelmodell og konfigurasjon
- gjennomgang av kjente feil, risikoer og teknisk gjeld
- besvarelse av rimelige spørsmål fra Kunden og ny leverandør

Kompetanseoverføringen skal dokumenteres.

6.6 Samarbeidsplikt

Leverandøren skal lojalt og aktivt medvirke til gjennomføringen av leverandørskiftet og bistå med nødvendige aktiviteter, overføringer og avklaringer i den utstrekning dette er nødvendig for å sikre en kontrollert overgang uten unødig avbrudd i tjenestene og uten tap av data, funksjonalitet, sikkerhet, sporbarhet eller revisjonsevne.

6.7 Testing av exit-plan

Kunden kan kreve gjennomføring av årlig exit-test, inkludert uttrekk av data, dokumentasjon og etablering av testmiljø hos tredjepart. Når Kunden finner det mer hensiktsmessig, kan exit-planen verifiseres gjennom en skrivebords øvelse som et alternativ til gjennomføring av exit-test.

Leverandøren skal uten ugrunnet opphold utbedre mangler som avdekkes gjennom slik verifikasjon.

7 Tredjepartsavhengigheter

Leverandøren skal identifisere, dokumentere og forvalte alle tredjepartsavhengigheter som inngår i eller er nødvendige for utvikling, drift, forvaltning og videreutvikling av løsningen.

Tredjepartsavhengigheter omfatter blant annet:

- tredjepartsprogramvare og -komponenter
- åpen kildekode (Open Source Software)
- biblioteker og rammeverk
- skyplattformer og skytjenester
- plattformtjenester og infrastrukturtjenester
- API-er og eksterne tjenester
- autentiserings- og sikkerhetstjenester
- meldingsformidlere og integrasjonskomponenter
- verktøy og tjenester som er nødvendige for bygging, testing, produksjonssetting og drift.

Leverandøren skal føre et oppdatert register over tredjepartsavhengigheter. Registeret skal som minimum beskrive:

- navn og versjon
- leverandør eller rettighetshaver
- funksjon og bruksområde
- berørte komponenter og integrasjoner
- lisensmodell
- supportstatus
- End-of-Support- og End-of-Life-datoer der dette er relevant
- identifiserte risikoer og sårbarheter
- avhengigheter til andre komponenter.

Registeret skal holdes løpende oppdatert og være tilgjengelig for Kunden gjennom hele avtaleperioden.