

TA-01-T

Vedlegg T - Systemadministrasjon

Nytt fagsystemet

GARANTIKASSEN FOR FISKERE

T.1 Formål og administrasjonsprinsipper	3
T.2 Administrative brukergrensesnitt	3
T.2.1 Generelle prinsipper	3
T.3 Konfigurasjonsadministrasjon	4
T.3.1 Generelle prinsipper for konfigurasjonsadministrasjon	4
T.3.2 Typer konfigurasjon	4
T.4 Operativ overvåkning og logghåndtering	5
T.4.1 Generelle prinsipper	5
T.5 Bruker- og tilgangsforvaltning	6
T.5.1 Generelle prinsipper	6
T.5.2 Administrasjon av brukere	6
T.5.3 Periodisk gjennomgang av tilganger	7
T.6 Batch-, jobb- og prosessadministrasjon	7
T.6.1 Generelle prinsipper for batch- og prosessadministrasjon	8
T.6.2 Kontroll og styring av prosesser	8
T.6.3 Gjennomføring og status	9
T.6.4 Feilhåndtering og re-prosessering	10
T.6.5 Kontroll og kvalitetssikring	10
T.6.6 Drift og tilgjengelighet	11
T.7 Integrasjonsadministrasjon	11
T.7.1 Generelle prinsipper for integrasjonsadministrasjon	12
T.7.1.1 API-baserte integrasjoner	12
T.7.1.2 Filbaserte integrasjoner	13
T.7.2 Status, overvåkning og varsling	13
T.7.3 Feilhåndtering og re-prosessering	15
T.7.4 Drift og tilgjengelighet	15
T.8 Systemvedlikehold og driftskontroll	16
T.8.1 Generelle prinsipper	16
T.8.2 Vedlikeholdsmodus og driftskontroll	16
T.9 Administrative rapporter og eksport	17
T.9.1 Generelle prinsipper	17

T.9.2 Rapportinnhold og presentasjon	17
T.9.3 Eksport og datauttrekk.....	18
T.9.4 Store rapporter og datauttrekk	18

T.1 Formål og administrasjonsprinsipper

Dette kapittelet beskriver overordnede prinsipper og krav for administrasjon, drift og kontroll av løsningen.

Formålet er å sikre at GFF kan administrere, overvåke og følge opp løsningen på en kontrollert og sporbar måte uten behov for databaseoperasjoner, kodeendringer eller direkte tilgang til underliggende infrastruktur.

Administrative funksjoner skal støtte:

- operativ drift
- kontroll og internoppfølging
- sikker administrasjon
- sporbarhet og revisjon
- konfigurasjonsforvaltning
- overvåkning og feilhåndtering
- administrativ rapportering

Administrative funksjoner skal støtte kontrollert separasjon mellom utviklings-, test-, akseptansetest- og produksjonsmiljø.

Administrative operasjoner i ett miljø skal ikke kunne påvirke andre miljøer utilsiktet.

T.2 Administrative brukergrensesnitt

Dette kapittelet beskriver krav til administrative brukergrensesnitt og arbeidsflater for drift, kontroll og administrasjon av løsningen.

Administrative arbeidsflater skal gjøre det mulig å utføre administrasjon, overvåkning, oppfølging og feilsøking uten behov for databaseoperasjoner eller tekniske spesialverktøy.

T.2.1 Generelle prinsipper

T.2.1.1 Løsningen skal tilby administrative brukergrensesnitt for operativ administrasjon og kontroll.

T.2.1.2 Administrative brukergrensesnitt skal være tilgjengelige gjennom standard nettleser.

T.2.1.3 Administrative arbeidsflater skal benytte konsistente prinsipper for navigasjon, søk, filtrering og presentasjon av data.

T.2.1.4 Administrative brukergrensesnitt skal støtte rollebasert tilgang.

T.2.1.5 Administrative funksjoner skal være dokumenterte og tilgjengelige for autoriserte brukere.

T.2.1.6 Administrative funksjoner skal kunne benyttes uten direkte tilgang til database eller operativsystem.

T.2.1.7 Administrative arbeidsflater skal støtte søk, filtrering og sortering.

T.2.1.8 Administrative arbeidsflater skal støtte eksport av søke- og rapportresultater til lesbare dokument- og dataformater.

T.2.1.9 Administrative arbeidsflater skal støtte presentasjon av systemstatus, prosessinformasjon og relevante driftsindikatorer.

T.3 Konfigurasjonsadministrasjon

Dette kapittelet beskriver krav til administrasjon, versjonering og kontrollert håndtering av konfigurasjon i løsningen.

Formålet er å sikre at GFF kan administrere og videreutvikle løsningens regelverk, parametere, prosesser og tekniske oppsett uten unødvendige kodeendringer eller leverandøravhengighet.

Dette vedlegget beskriver administrative funksjoner for å forvalte konfigurasjon. Selve regelmodellens struktur, regeltypen, parametere og evaluering er beskrevet i vedlegg TA-01-L.

T.3.1 Generelle prinsipper for konfigurasjonsadministrasjon

T.3.1.1 Løsningen skal støtte administrasjon av konfigurasjon gjennom dedikerte administrative funksjoner.

T.3.1.2 Konfigurasjonsendringer skal som hovedregel kunne utføres uten databaseoperasjoner eller kodeendringer.

T.3.1.3 Konfigurasjonsadministrasjon skal være rollebasert og underlagt tilgangskontroll.

T.3.1.4 Konfigurasjonsadministrasjon skal være konsistent på tvers av moduler og fagområder.

T.3.1.5 Administrative funksjoner for konfigurasjon skal være dokumenterte og tilgjengelige for autoriserte brukere.

T.3.1.6 Løsningen skal støtte validering av konfigurasjon før aktivering.

T.3.1.7 Løsningen skal støtte håndtering av relaterte konfigurasjonsendringer som én samlet konfigurasjonspakke.

T.3.2 Typer konfigurasjon

T.3.2.1 Løsningen skal støtte administrasjon av:

- satser
- terskelverdier
- kodeverk
- regelparametere
- batchparametere
- integrasjonsparametere
- dokumentrelaterte parametere
- prosessparametere

T.3.2.2 Løsningen skal støtte ordningsspesifikk konfigurasjon.

T.3.2.3 Løsningen skal støtte miljøspesifikk konfigurasjon uten å påvirke historiske vedtak eller tidligere behandlinger.

T.3.2.4 Løsningen skal støtte tidsstyrt aktivering av konfigurasjon.

T.3.2.5 Miljøspesifikk konfigurasjon skal ikke endre faglig regelverk eller beregningslogikk uten at dette er definert som egen regel- eller konfigurasjonsversjon.

T.4 Operativ overvåkning og logghåndtering

Dette kapittelet beskriver krav til felles logg-, hendelses- og sporingsinformasjon for administrativ oppfølging av løsningen.

Formålet er å sikre at GFF kan overvåke, analysere og følge opp drift, batchprosesser, integrasjoner og systemhendelser på en kontrollert og effektiv måte.

Krav til sikkerhetslogging, audit, journalføring og revisjonsspor er beskrevet i vedleggene TA-01-B, TA-01-C og TA-01-D.

T.4.1 Generelle prinsipper

T.4.1.1 Løsningen skal støtte samlet administrativ tilgang til logger, hendelser og prosessinformasjon på tvers av moduler og integrasjoner.

T.4.1.2 Logger og hendelser skal kunne presenteres gjennom administrative arbeidsflater.

T.4.1.3 Løsningen skal støtte søk, filtrering og analyse av logger og hendelser.

T.4.1.4 Logger og hendelser skal kunne korreleres og spores på tvers av batchprosesser, integrasjoner og distribuerte eller relaterte systemhendelser.

T.4.1.5 Løsningen skal støtte korrelasjons- eller sporingsidentifikatorer som gjør det mulig å følge relaterte hendelser, batchprosesser og integrasjoner på tvers av systemkomponenter.

T.4.1.6 Administrative arbeidsflater skal støtte skjerming eller pseudonymisering av sensitive identifikatorer der full identitet ikke er nødvendig for arbeidsoppgaven.

T.4.1.7 Løsningen skal støtte kontrollert håndtering av oppbevaringstid for logger og hendelser basert på loggtype, sikkerhetsbehov, revisjonskrav eller regulatoriske krav.

T.4.1.8 Logger og hendelser skal benytte konsistent tidsgrunnlag på tvers av systemkomponenter.

T.4.1.9 Operative logger og hendelser skal beskyttes mot utilsiktet endring eller sletting.

T.5 Bruker- og tilgangsförvaltning

Dette kapittelet beskriver krav til administrativ förvaltning av brukere, roller og tilganger i løsningen.

Formålet er å sikre at GFF kan administrere og følge opp brukertilgang på en kontrollert, sporbar og effektiv måte.

Krav til autentisering, identitetsdomener, autorisasjonsmodell og sikkerhetsarkitektur er beskrevet i vedleggene TA-01-B og TA-01-C.

T.5.1 Generelle prinsipper

T.5.1.1 Løsningen skal støtte administrativ håndtering av brukere, roller og tilganger gjennom dedikerte administrative arbeidsflater.

T.5.1.2 Administrative funksjoner for bruker- og tilgangsförvaltning skal være tilgjengelige uten databaseoperasjoner eller kodeendringer.

T.5.1.3 Administrasjon av brukere og tilganger skal være rollebasert og underlagt tilgangskontroll.

T.5.1.4 Administrative arbeidsflater skal være konsistente på tvers av moduler og fagområder.

T.5.1.5 Administrative funksjoner for bruker- og tilgangsförvaltning skal være dokumenterte og tilgjengelige for autoriserte brukere.

T.5.1.6 Løsningen skal støtte delegasjon av administrative oppgaver basert på rolle og ansvarsområde.

T.5.1.7 Tilganger skal som hovedregel tildeles etter prinsippet om minste privilegium.

T.5.2 Administrasjon av brukere

T.5.2.1 Løsningen skal støtte opprettelse, vedlikehold, sperring, deaktivering og reaktivering av brukere.

T.5.2.2 Løsningen skal støtte administrasjon av både interne og eksterne brukere der dette er relevant.

T.5.2.3 Brukere skal kunne knyttes til roller, grupper, organisatoriske enheter eller fagområder.

T.5.2.4 Løsningen skal støtte søk og oppslag på brukere.

T.5.2.5 Deaktiverte brukere skal ikke miste historiske referanser i logger, saker eller prosesser.

T.5.2.6 Endringer i brukerstatus og tilknytning skal være sporbare.

T.5.2.7 Løsningen skal støtte midlertidig sperring eller begrensning av brukertilgang.

T.5.2.8 Nye brukere skal som hovedregel ikke tildeles privilegerte tilganger automatisk.

T.5.2.9 Løsningen skal støtte administrativ terminering eller sperring av aktive brukerøker der dette er relevant.

T.5.2.10 Løsningen skal støtte identifisering av brukere uten gyldig organisatorisk tilknytning eller rolle.

T.5.2.11 Løsningen skal støtte identifisering og administrativ oppfølging av tekniske brukere, tjenestekontoer og andre systemidentiteter.

T.5.2.12 Bruk av generiske eller delte brukeridentiteter skal som hovedregel unngås. Der slike identiteter er teknisk nødvendige, skal formål, ansvar og tildelte rettigheter være dokumentert og bruken være sporbar.

T.5.2.13 Privilegerte brukere og systemidentiteter med utvidede rettigheter skal kunne identifiseres særskilt for kontroll og revisjon.

T.5.3 Periodisk gjennomgang av tilganger

Dette delkapittelet beskriver krav til kontroll og etterprøving av etablerte brukertilganger. Formålet er å sikre at tildelte roller og rettigheter fortsatt er nødvendige og korrekte over tid.

T.5.3.1 Løsningen skal støtte periodisk gjennomgang av brukere, roller og tildelte tilganger.

T.5.3.2 Løsningen skal gjøre det mulig å identifisere og kontrollere privilegerte tilganger, brukere uten gyldig organisatorisk tilknytning og andre tilganger som krever særskilt oppfølging.

T.5.3.3 Gjennomført tilgangsgjennomgang skal kunne dokumenteres med tidspunkt, ansvarlig bruker og resultat av gjennomgangen.

T.5.3.4 Endringer som følger av tilgangsgjennomgang skal være sporbare i samsvar med kravene til logging og revisjon.

T.6 Batch-, jobb- og prosessadministrasjon

Dette kapittelet beskriver krav til administrativ oppfølging og kontroll av automatiserte prosesser i løsningen.

Formålet er å sikre at GFF kan overvåke, følge opp og kontrollere automatiserte prosesser på en trygg og effektiv måte, uten å være avhengig av databaseoperasjoner, kodeendringer eller direkte tilgang til underliggende teknisk infrastruktur.

Løsningen skal støtte operativ kontroll og oppfølging av blant annet:

- batchprosesser
- beregningskjøringer
- import- og eksportprosesser
- dokumentproduksjonsprosesser
- betalings- og oppgjørsrelaterte prosesser
- automatiserte integrasjonsprosesser
- feiloppfølging og re-prosessering

Krav til logging, overvåkning og loggsøk er beskrevet i kapittel T.4. Krav til økonomiske utbetalings- og oppgjørsprosesser er beskrevet i vedlegg TA-01-K.

T.6.1 Generelle prinsipper for batch- og prosessadministrasjon

T.6.1.1 Løsningen skal støtte administrativ oppfølging av automatiserte prosesser gjennom administrative arbeidsflater eller integrasjon mot egnet drifts- eller overvåkningsverktøy.

T.6.1.2 Løsningen skal gi autoriserte brukere innsikt i status, fremdrift og resultat for automatiserte prosesser.

T.6.1.3 Automatiserte prosesser skal kunne identifiseres med relevant informasjon, herunder navn, type, tidspunkt, status og prosessreferanse der dette er relevant.

T.6.1.4 Løsningen skal støtte rollebasert tilgang til administrasjon og oppfølging av automatiserte prosesser.

T.6.1.5 Løsningen skal støtte samlet oversikt over aktive, planlagte, fullførte, feilede og avbrutte prosesser.

T.6.1.6 Løsningen skal støtte søk og filtrering i prosesshistorikk og statusinformasjon.

T.6.1.7 Løsningen skal støtte identifisering av prosesser som er forsinket, feilet eller ikke fullført som forventet.

T.6.2 Kontroll og styring av prosesser

Dette delkapittelet beskriver krav til kontrollert styring og oppfølging av automatiserte prosesser.

Løsningen skal gi GFF tilstrekkelig kontroll over prosesser som påvirker behandling, beregning, dokumentproduksjon eller økonomiske hendelser.

T.6.2.1 Løsningen skal støtte kontrollert oppstart av automatiserte prosesser der dette er relevant.

T.6.2.2 Løsningen skal støtte kontrollert stopp eller avbrytelse av prosesser for autoriserte brukere der dette er relevant.

T.6.2.3 Løsningen skal støtte midlertidig deaktivering eller sperring av automatiserte prosesser der dette er relevant.

T.6.2.4 Endringer i status, aktivering eller styring av automatiserte prosesser skal være sporbare.

T.6.2.5 Manuell oppstart, stopp eller re-prosessering skal loggføres med bruker, tidspunkt og relevant kontekst.

T.6.2.6 Løsningen skal støtte kontrollmekanismer som reduserer risiko for utilsiktet dobbeltkjøring eller duplikatbehandling.

T.6.2.7 Løsningen skal støtte kontrollert håndtering av prosesser som er avhengige av tidligere behandling eller relaterte prosesser der dette er nødvendig for konsistent behandling.

T.6.3 Gjennomføring og status

Dette delkapittelet beskriver krav til statusoppfølging og operativ innsikt i automatiserte prosesser.

Løsningen skal gjøre det mulig å følge opp fremdrift, resultat og feilstatus for relevante prosesser.

T.6.3.1 Løsningen skal kunne vise status for automatiserte prosesser.

T.6.3.2 Status skal minimum kunne indikere om en prosess er:

- planlagt
- startet
- under behandling
- fullført
- feilet
- avbrutt
- pauset der dette er relevant
- re-prosessert

T.6.3.3 Løsningen skal kunne vise tidspunkt for start og slutt samt resultatstatus for gjennomførte prosesser.

T.6.3.4 Løsningen skal støtte presentasjon av relevante feilmeldinger og

avviksinformasjon.

T.6.3.5 Løsningen skal støtte sporbar kobling mellom prosesser og tilhørende:

- batcher
- vedtak
- dokumentproduksjon
- integrasjonshendelser
- økonomiske transaksjoner

T.6.3.6 Løsningen skal støtte identifisering av delvis gjennomførte eller ufullstendige prosesser.

T.6.4 Feilhåndtering og re-prosessering

Dette delkapittelet beskriver krav til håndtering av feil, avvik og kontrollert re-prosessering.

Løsningen skal støtte trygg og sporbar håndtering av feil uten å skape inkonsistente data eller utilsiktede duplikater.

T.6.4.1 Løsningen skal støtte identifisering og oppfølging av feilede prosesser.

T.6.4.2 Løsningen skal støtte kontrollert re-prosessering der dette er relevant.

T.6.4.3 Re-prosessering skal være sporbar.

T.6.4.4 Re-prosessering skal ikke kunne omgå kontrollmekanismer for sporbarhet, duplikatkontroll eller økonomisk kontroll.

T.6.4.5 Løsningen skal støtte at feil i enkeltprosesser kan håndteres uten at øvrige prosesser nødvendigvis påvirkes.

T.6.4.6 Løsningen skal støtte administrativ oppfølging av avvik og feilsituasjoner.

T.6.5 Kontroll og kvalitetssikring

Dette delkapittelet beskriver krav til kontroll og kvalitetssikring av automatiserte prosesser.

Automatiserte prosesser skal kunne etterprøves og kontrolleres som del av ordinær drift og revisjon.

T.6.5.1 Løsningen skal støtte sporbarhet for gjennomførte prosesser.

T.6.5.2 Løsningen skal støtte dokumentasjon av prosessresultater der dette er relevant.

T.6.5.3 Løsningen skal støtte kontroll av at prosesser er gjennomført i henhold til definert behandlingsgrunnlag.

T.6.5.4 Løsningen skal støtte identifisering av avvik eller manglende behandling.

T.6.5.5 Løsningen skal støtte sammenhengende sporbarhet mellom prosesser, vedtak,

dokumenter og økonomiske hendelser der dette er relevant.

T.6.6 Drift og tilgjengelighet

Dette delkapittelet beskriver krav til robusthet og operativ tilgjengelighet knyttet til automatiserte prosesser.

T.6.6.1 Løsningen skal støtte stabil og kontrollert gjennomføring av automatiserte prosesser.

T.6.6.2 Løsningen skal støtte håndtering av midlertidige feil uten tap av sporbarhet eller prosesshistorikk.

T.6.6.3 Løsningen skal støtte overvåkning og administrativ oppfølging av prosesser uten behov for direkte tilgang til underliggende infrastruktur.

T.6.6.4 Administrative funksjoner for prosessoppfølging skal være tilgjengelige for autoriserte brukere gjennom standard administrative arbeidsflater eller egnet driftsverktøy.

T.7 Integrasjonsadministrasjon

Dette kapittelet beskriver krav til administrativ oppfølging, kontroll og overvåkning av integrasjoner og datautveksling mellom løsningen og eksterne systemer.

Formålet er å sikre at GFF kan følge opp integrasjoner, identifisere feil og avvik, samt gjennomføre kontrollert oppfølging og re-prosessering uten behov for databaseoperasjoner, kodeendringer eller direkte tilgang til underliggende teknisk infrastruktur.

Kapittelet omfatter administrativ oppfølging av blant annet:

- API-baserte integrasjoner
- filbaserte integrasjoner
- meldingsbaserte integrasjoner
- import- og eksportprosesser
- synkronisering av registerdata
- økonomiske overføringer
- status- og kvitteringsmeldinger

Krav til sikkerhet, autentisering og autorisasjon for integrasjoner er beskrevet i vedleggene TA-01-B, TA-01-C og TA-01-Q. Krav til økonomiske integrasjoner og oppgjørprosesser er beskrevet i vedlegg TA-01-K.

T.7.1 Generelle prinsipper for integrasjonsadministrasjon

Dette delkapittelet beskriver overordnede prinsipper for administrasjon og kontroll av integrasjoner.

Integrasjonsadministrasjon skal støtte kontrollert drift, feiloppfølging og sporbar kommunikasjon mellom systemer.

T.7.1.1 API-baserte integrasjoner

Dette delkapittelet beskriver krav til administrativ oppfølging av API-baserte integrasjoner.

Løsningen skal gi GFF innsikt i relevante konfigurasjons- og statusopplysninger for API-baserte integrasjoner, inkludert oppfølging av sertifikater, tilkoblingsstatus og kontrollert testing av integrasjoner.

T.7.1.1.1 Løsningen skal støtte administrativ oversikt over relevante konfigurasjonsparametere for API-baserte integrasjoner.

T.7.1.1.2 Løsningen skal kunne vise informasjon om:

- integrasjonsnavn
- endpoint eller tjenestereferanse
- status
- tidspunkt for siste vellykkede kommunikasjon
- relevante sertifikater der dette benyttes

T.7.1.1.3 Løsningen skal der det er relevant støtte kontrollert testing av API-baserte integrasjoner gjennom ping, helsesjekk eller tilsvarende ikke-funksjonelle testkall (NO OP).

T.7.1.1.4 Løsningen skal støtte administrativ oppfølging av sertifikater brukt i integrasjoner, herunder:

- gyldighetsperiode
- utløpsdato
- status

T.7.1.1.5 Løsningen skal støtte kontrollert oppdatering eller utskifting av integrasjonssertifikater der dette er relevant.

T.7.1.1.6 Sensitive autentiseringsopplysninger skal håndteres på en sikker måte og skal ikke eksponeres i klartekst i administrative arbeidsflater.

T.7.1.2 Filbaserte integrasjoner

Dette delkapittelet beskriver krav til administrativ oppfølging av filbaserte integrasjoner og datautvekslinger.

Løsningen skal gi GFF innsikt i relevante konfigurasjons- og statusopplysninger for filbaserte integrasjoner, inkludert oppfølging av filoverføringer, sikkerhetsrelatert konfigurasjon og kontrollert testing av tilkobling der dette er relevant.

T.7.1.2.1 Løsningen skal støtte administrativ oversikt over filbaserte integrasjoner og datautvekslinger.

T.7.1.2.2 Løsningen skal kunne vise relevant konfigurasjonsinformasjon for filbaserte integrasjoner, herunder:

- filområder eller katalogreferanser
- filnavnmønster der dette er relevant
- overføringsretning
- tidspunkt for siste mottatte eller overførte fil
- status for siste filoverføring

T.7.1.2.3 Løsningen skal der det er relevant støtte kontrollert testing av filbaserte integrasjoner eller tilkoblinger, herunder validering av tilgjengelighet, autentisering eller kommunikasjonsstatus.

T.7.1.2.4 Løsningen skal støtte kontrollert vedlikehold av konfigurasjon for filbaserte integrasjoner der dette er relevant.

T.7.1.2.5 Løsningen skal støtte administrativ oppfølging av sertifikater, autentiseringsmekanismer eller tilsvarende sikkerhetskongfigurasjon for filbaserte integrasjoner.

T.7.1.2.6 Sensitive autentiseringsopplysninger skal håndteres på en sikker måte og skal ikke eksponeres i klartekst i administrative arbeidsflater.

T.7.2 Status, overvåkning og varsling

Dette delkapittelet beskriver krav til statusoppfølging, overvåkning og operativ varsling knyttet til integrasjoner og datautveksling.

Løsningen skal gi autoriserte brukere innsikt i tilgjengelighet, status, feil og hendelser knyttet til integrasjoner mot interne og eksterne systemer.

T.7.2.1 Løsningen skal støtte operativ overvåkning og oppfølging av integrasjoner og datautvekslinger.

T.7.2.2 Løsningen skal kunne vise relevant statusinformasjon for integrasjoner, herunder:

- teknisk eller funksjonell status der dette er relevant
- tilgjengelighet
- tidspunkt for siste vellykkede overføring
- tidspunkt for siste feilede overføring
- feilstatus
- relevante hendelser og avvik

T.7.2.3 Kritiske feil og avvik skal kunne identifiseres gjennom varslings-, statusindikatorer eller administrative oversikter.

T.7.2.4 Løsningen skal støtte administrative dashboards eller oversiktsbilder for operativ oppfølging av integrasjoner og relaterte prosesser.

T.7.2.5 Løsningen skal støtte historikk og sporbarhet for integrasjonshendelser der dette er relevant.

T.7.2.6 Autoriserte brukere skal kunne se relevant feilkontekst og hendelsesinformasjon der dette er nødvendig for oppfølging og feilsøking.

T.7.2.7 Løsningen skal støtte sammenhengende sporbarhet mellom integrasjonshendelser, relaterte prosesser og relevante forretningshendelser der dette er relevant.

T.7.2.8 Løsningen skal støtte konfigurert varslings- og drifts- og integrasjonshendelser.

T.7.2.9 Varsling skal kunne benyttes for blant annet:

- feilede integrasjoner
- avviste eller ufullstendige datautvekslinger
- fullførte batchprosesser
- fullført dokumentproduksjon
- gjennomførte import- eller eksportprosesser
- kritiske feil eller avvik

T.7.2.10 Varsling skal kunne distribueres via e-post.

T.7.2.11 Løsningen skal støtte konfigurert mottakerliste for varsling.

T.7.2.12 Varsling skal kunne differensieres basert på type hendelse, alvorlighetsgrad eller prosess der dette er relevant.

T.7.2.13 Varsling skal ikke føre til utilsiktet eksponering av sensitive opplysninger.

T.7.2.14 Løsningen skal støtte sporbarhet for utsendte varsler der dette er relevant.

T.7.3 Feilhåndtering og re-prosessering

Dette delkapittelet beskriver krav til kontrollert håndtering av integrasjonsfeil og oppfølging av avvik.

Løsningen skal støtte trygg og sporbar håndtering av feil uten å skape utilsiktede duplikater eller inkonsistente resultater.

T.7.3.1 Løsningen skal støtte identifisering og oppfølging av feilede integrasjonshendelser.

T.7.3.2 Feilede integrasjonshendelser skal kunne følges opp gjennom administrative arbeidsflater eller egnet driftsverktøy.

T.7.3.3 Løsningen skal støtte kontrollert re-prosessering der dette er relevant.

T.7.3.4 Re-prosessering skal være rollebasert og begrenset til autoriserte brukere.

T.7.3.5 Re-prosessering skal være sporbar og kunne knyttes til opprinnelig hendelse eller prosess der dette er relevant.

T.7.3.6 Re-prosessering skal ikke kunne omgå kontrollmekanismer for sporbarhet, idempotens, duplikatkontroll eller økonomisk kontroll.

T.7.3.7 Løsningen skal støtte kontrollert håndtering av enkeltstående feil uten at øvrige integrasjoner nødvendigvis påvirkes.

T.7.3.8 Det skal være mulig å registrere relevant begrunnelse eller kontekst ved manuell re-prosessering der dette er relevant.

T.7.3.9 Løsningen skal støtte identifisering og administrativ oppfølging av integrasjonshendelser som ikke kan behandles automatisk.

T.7.4 Drift og tilgjengelighet

Dette delkapittelet beskriver krav til operativ tilgjengelighet og stabil bruk av integrasjonsadministrative funksjoner.

Administrative funksjoner for integrasjoner skal støtte kontrollert og stabil oppfølging av integrasjoner og datautvekslinger uten å påvirke ordinær saksbehandling unødvendig.

T.7.4.1 Administrative funksjoner for integrasjonsoppfølging skal være tilgjengelige i relevante miljøer.

T.7.4.2 Løsningen skal støtte kontrollert samtidig bruk av integrasjonsadministrative

funksjoner for autoriserte brukere.

T.7.4.3 Integrasjonsadministrasjon skal kunne benyttes uten å påvirke ordinær saksbehandling unødvendig.

T.7.4.4 Løsningen skal være dimensjonert for forventet omfang av integrasjoner og datautvekslinger.

T.8 Systemvedlikehold og driftskontroll

Dette kapittelet beskriver krav til kontrollert vedlikehold og operativ driftskontroll av løsningen.

Formålet er å sikre at GFF kan gjennomføre planlagt vedlikehold, håndtere driftsavvik og følge opp redusert tilgjengelighet på en kontrollert og sporbar måte.

Krav til backup, gjenoppretting og beredskap er beskrevet i vedleggene TA-01-C og TA-01-Q.

T.8.1 Generelle prinsipper

Dette delkapittelet beskriver overordnede prinsipper for systemvedlikehold og driftskontroll.

Administrative driftsfunksjoner skal støtte stabil, kontrollert og forutsigbar drift av løsningen.

T.8.1.1 Løsningen skal støtte administrative funksjoner for systemvedlikehold og driftskontroll.

T.8.1.2 Administrative driftsfunksjoner skal være rollebaserte og underlagt tilgangskontroll.

T.8.2 Vedlikeholdsmodus og driftskontroll

Dette delkapittelet beskriver krav til kontrollert vedlikehold og håndtering av driftsavvik.

Løsningen skal støtte kontrollert gjennomføring av vedlikehold uten unødvendig risiko for datatap, inkonsistent behandling eller utilsiktede avbrudd i kritiske prosesser.

T.8.2.1 Løsningen skal støtte vedlikeholdsmodus der dette er relevant.

T.8.2.2 Vedlikeholdsmodus skal kunne begrense eller stanse nye behandlinger og prosesser på en kontrollert måte.

T.8.2.3 Aktivering og deaktivering av vedlikeholdsmodus skal være sporbar.

T.8.2.4 Løsningen skal støtte administrative meldinger eller statusindikatorer ved vedlikehold eller driftsavvik.

T.8.2.5 Løsningen skal støtte kontrollert drift ved delvis utilgjengelige integrasjoner eller komponenter der dette er relevant.

T.9 Administrative rapporter og eksport

Dette kapittelet beskriver krav til administrative rapporter, eksportfunksjoner og operativ dokumentasjon.

Formålet er å sikre at GFF kan generere, eksportere og følge opp administrative data, kontrollrapporter og driftsinformasjon på en kontrollert og lesbar måte.

Krav til dokumentproduksjon, dokumentformat og rapportutforming er beskrevet nærmere i vedlegg TA-01-O.

T.9.1 Generelle prinsipper

Dette delkapittelet beskriver overordnede prinsipper for administrative rapporter og eksportfunksjoner.

Administrative rapporter skal støtte:

drift og oppfølging

kontroll og kvalitetssikring

revisjon og internkontroll

feilsøking og analyse

dokumentasjon av administrative aktiviteter

T.9.1.1 Løsningen skal støtte generering av administrative rapporter og relevante datauttrekk.

T.9.1.2 Rapporter skal kunne genereres både manuelt og som del av automatiserte prosesser.

T.9.1.3 Administrative rapporter skal være rollebaserte og underlagt tilgangskontroll.

T.9.2 Rapportinnhold og presentasjon

Dette delkapittelet beskriver krav til innhold og presentasjon av administrative rapporter.

T.9.2.1 Administrative rapporter skal kunne presenteres i standard dokument- eller dataformat egnet for lesing, kontroll og oppfølging.

T.9.2.2 Administrative rapporter og oppslag skal støtte skjerming eller pseudonymisering av sensitive identifikatorer i både visning, eksport og datauttrekk der dette er relevant.

T.9.2.3 Administrative rapporter skal kunne inneholde informasjon som gjør det mulig å kontrollere rapportens opprinnelse og genereringstidspunkt.

T.9.2.4 Rapporter skal støtte søk, filtrering og sortering der dette er relevant.

T.9.2.5 Administrative rapporter og datauttrekk skal kunne benyttes som

dokumentasjonsgrunnlag for internkontroll og revisjon, herunder for kontroll av brukere, tilganger, administrative endringer og relevante systemhendelser.

T.9.3 Eksport og datauttrekk

Dette delkapittelet beskriver krav til eksport og administrative datauttrekk.

T.9.3.1 Løsningen skal støtte eksport av administrative rapporter og datauttrekk til relevante dokument- og dataformater, herunder PDF og Excel der dette er hensiktsmessig.

T.9.3.2 Eksport og datauttrekk skal være sporbare med bruker, tidspunkt og eksporttype.

T.9.3.3 Løsningen skal kunne begrense eksport av sensitive administrative data basert på rolle, datakategori og tilgangsnivå.

T.9.3.4 Store rapporter og eksportjobber skal kunne genereres asynkront der dette er relevant.

T.9.4 Store rapporter og datauttrekk

Dette delkapittelet beskriver krav til kontrollert bruk og tilgjengelighet for rapport- og eksportfunksjoner.

T.9.4.1 Løsningen skal støtte kontrollert håndtering av store rapporter og datauttrekk.