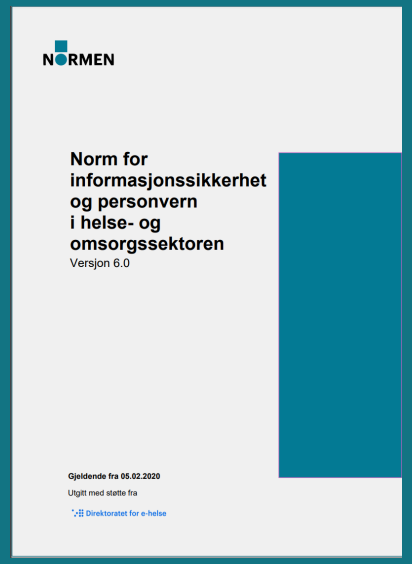
Veileder for leverandører til helse- og omsorgssektoren

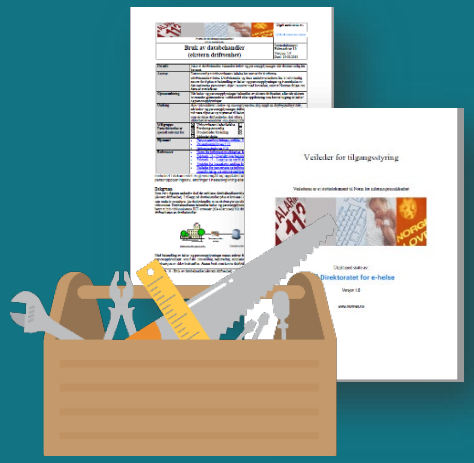
04.10.23

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren

Bransjenormen



Veiledning



Arena

Normkonferansen 2019

Norges første og største bransjenorm for informasjonssikkerhet – og fra 2018 også for personvern

NORMEN

Normkonferansen

NOV | 21–22 | 2023

The Qube, Gardermoen

SKANN MEG

Bli med på kurs på Pre-Normkonferansen

Program for Normkonferansen

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren

Normen er til for..

.. **alle virksomheter** som ved **avtale** har forpliktet seg til å følge **Normen –** i praksis de fleste av sektorens mer enn titusen virksomheter og deres leverandører og databehandlere

Normen godkjennes og forvaltes av..

KS · Den norske legeforening · Apotekforeningen · Norges Farmaceutiske Forening · KiNS · Den norske tannlegeforening · folkehelseinstituttet · Helse Midt-Norge · Helse Nord · Helse Vest · Helse Sør-Øst · Helsedirektoratet · Direktoratet for e-helse · norskhelsenett

Den offentlige tannhelsetjeneste

nav · Digdir · FFO · IKT Norge · Melanor · NSM

.. en bredt sammensatt **styringsgruppe** fra sektoren

Normens daglige arbeid koordineres av..

Direktoratet for e-helse

norskhelsenett

.. et **sekretariat** plassert i Direktoratet for e-helse med fast representasjon fra Norsk Helsenett

Styringsgruppen for Normen

Helse- og omsorgsdepartementet

Direktoratet for e-helse

Sekretariatet for Normen

NORMEN

- Sekretariatsfunksjon
- Utvikler veiledning
- Kompetanseheving og utadrettet virksomhet

Fagorgan

- Utredninger
- Deltar i prosjekter og fora i/ for direktoratet
- Direktoratsfunksjon

Seksjon Informasjonssikkerhet

Styringsgruppen for Normen

MEDLEMMER

- Apotekforeningen
- Den norske legeforening
- Den norske tannlegeforening
- Norsk farmaceutisk forening
- Norsk fysioterapeutforbund
- Norsk psykologforening
- Norsk sykepleierforbund
- KS
- KiNS
- Helse Midt-Norge RHF
- Helse Nord RHF
- Helse Sør-Øst RHF
- Helse Vest RHF
- *Fûrst (Private helsevirksomheter)*
- Folkehelseinstituttet
- Direktoratet for e-helse
- Helsedirektoratet
- Norsk Helsenett

OBSERVATØRER

- Digitaliseringsdirektoratet
- NAV
- *NSM*
- *IKT Norge (Leverandørorganisasjoner)*
- *Melanor (Leverandørorganisasjoner)*
- *FFO – funksjonshemmedes fellesorganisasjon (Pasientorganisasjoner)*
- *Senior Norge (Pasientorganisasjoner)*
- *We Shall Overcome (Pasientorganisasjoner)*

Andre aktiviteter i regi av Normen

Normkonferansen

22-23. November
The Qube, Gardermoen

Nyhetsbrev

- Ca. en gang i måneden
- Påmelding www.ehelse.no

Q&A epost

sikkerhetsnormen@ehelse.no

Kurs og webinar

- Kurs
- Webinarer
- Konferanser
- Foredrag

www.normen.no

- Alle dokumentene
- Nyheter
- Om Normen
- Påmelding til kurs og webinar

Sosiale medier

Følg oss på FB og LinkedIn!

NORMEN

Normkonferansen

NOV | 21-22 | 2023

The Qube, Gardermoen

SKANN MEG

Bli med på kurs på Pre-Normkonferansen

Program for Normkonferansen

Veileder for Informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

- Godkjent av Styringsgruppen for Normen 08.06.23

- Veilederen beskriver tiltak og forventninger til IKT-løsninger, medisinsk utstyr og operasjonell teknologi (OT) fra leverandørens perspektiv.
  - To vedlegg
    - HUKI-Matrise
    - Flytskjema som viser innføringsprosess

- Referansegruppe bestående av:
  - IT-leverandør til sektoren
  - Flere leverandører av Medisinsk utstyr
  - Driftsorganisasjoner innen spesialist (IT og med-tek)
  - Sykehusinnkjøp og Norsk helsenett
  - Innkjøpskompetanse i kommune

NORMEN

Informasjonssikkerhet og personvern – sett fra mange leverandørers ståsted

Alt for komplisert

Alt for strenge krav

Usikkerhet hva som gjelder for «oss»

Hjelp… for noe kjedelig opplegg

Det er jo sånn lover og greier, det får noen andre ta seg av

Typiske krav som stilles i forbindelse med anskaffelser

- Normen skal følges
- Leverandøren skal følge Normen
- Normens samlete krav skal besvares (294 stk.)
- Leverandøren skal ha et styringssystem for Informasjonssikkerhet og personvern
- Oppdragsgivers fjernaksessløsning SKAL benyttes

- «Løsningen må være egnet til å ivareta relevante krav som stilles i den til enhver tid gjeldende Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen).»

Målgruppe

- Målgruppen er leverandører til helse og omsorgstjenesten, og ansatte hos virksomheter i helse- og omsorgstjenesten som forvalter og anskaffer teknologi og programvare.

- Målgruppen for veilederen er virksomheter som omfattes av Normen og som skal sikre etterlevelse av Normens krav, herunder dataansvarlig.

- Veilederen kan også være nyttig for systemleverandører og andre samarbeidspartnere til helse- og omsorgssektoren, som på grunn av sin leveranse eller engasjement er omfattet av Normen gjennom avtale med virksomheten eller Norsk Helsenett SF.

Veilederens innhold

Personvern, informasjonssikkerhet og taushetsplikt

- Er leverandør det samme som databehandler?
- Noen utvalgte personvernområder
- Personvernprinsippene
- Formål og behandlingsgrunnlag
- De registrertes rettigheter
- Innebygget personvern
- Taushetsplikt om helse og personopplysninger

Ansvar for å følge kravene i Normen

Den dataansvarlige har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden.
I leveranser av f.eks. tjenester, maskinvare eller systemer skal det avtales skriftlig med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar.

Hvilke av Normens krav som gjennom avtale gjelder for leverandører, er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- Databehandling, i form av for eksempel skytjenester eller driftstjenester
- Vedlikehold, for eksempel ved fysisk service eller fjernaksess
- Leveranse av løsninger og systemer

Risiko

- Risikovurdering (ROS)
- Personvernkonsekvensvurdering (DPIA)

Avtaler og krav til oversikt og kontroll

- Styringssystem/ internkontroll
- Protokoll (GDPR)
- Kontrakt
- Databehandleravtaler

Anbefalinger og krav til IKT og tekniske løsninger

- Når blir et system å anse som medisinsk utstyr?
- Løsninger som benytter skytjenester
- Særlig om systemer som behandler helse- og personopplysninger
- Sikkerhetskrav til programmeringsgrensesnitt
- Utprøving og utlån av utstyr
- Sletting av opplysninger

Anbefalte tiltak i forbindelse med etablering av nye systemer og oppgradering/migrering av eksisterende systemer

- Ansvar for de forskjellige delene av prosessen
- HUKI-matrise

Lokalt installert programvare/systemer hos kunden

- Sikkerhetsutfordringer knyttet til løsninger som kjører lokalt hos kunden, og avhengighet av slike systemer.

- styring av heis
- adgangssystem
- styringssystemer for strøm, vann og ventilasjon.
- medisinsk utstyr
- lokalt installerte servere
- lokalt installert programvare

Utstyr plassert hjemme hos pasient/bruker

- Sikkerhetsutfordringer hjemme hos pasienter

- Ustabil nettverksforbindelse (bredbånd og mobilnett)
- Usikker strømforsyning
- Mulig uautorisert tilgang til utstyret, som kan føre til uønskede endringer, for eksempel endring av alarmgrenser
- Manglende forståelse eller adekvat håndtering av alarmer fra brukeren, som for eksempel:
  - batteribytte i trygghetsalarm
- Er teknologien egnet for pasientgruppen den er tiltenkt
- Manglende tilgjengelighet av opplysninger for helsepersonell

Tilgang til utstyr plassert hos kunden

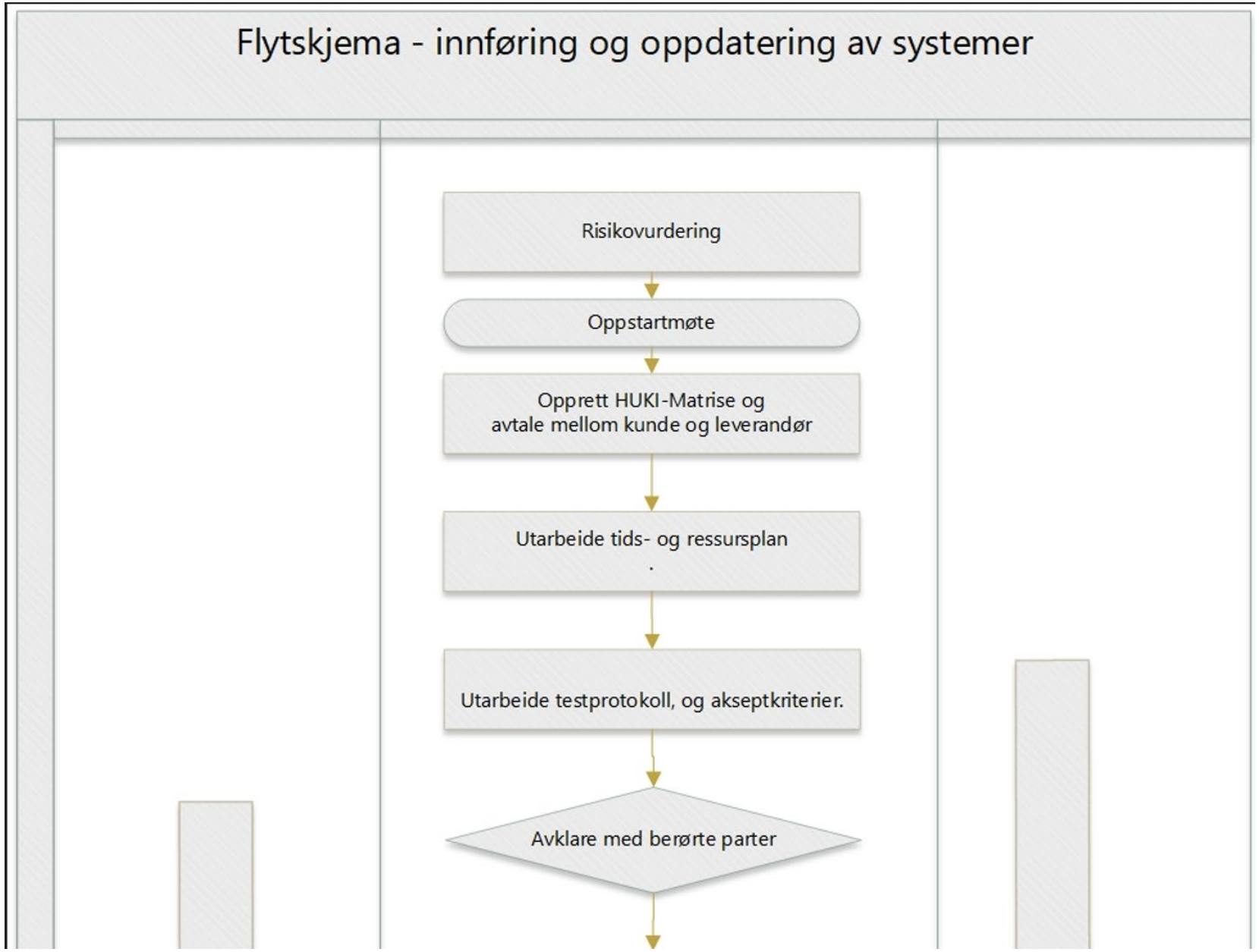
- Fjernaksess
- Reparasjon og service på utstyr plassert hos kunden
- Håndtering av utstyr mottatt fra kunden for service\reparasjon\destruksjon som inneholder personopplysninger

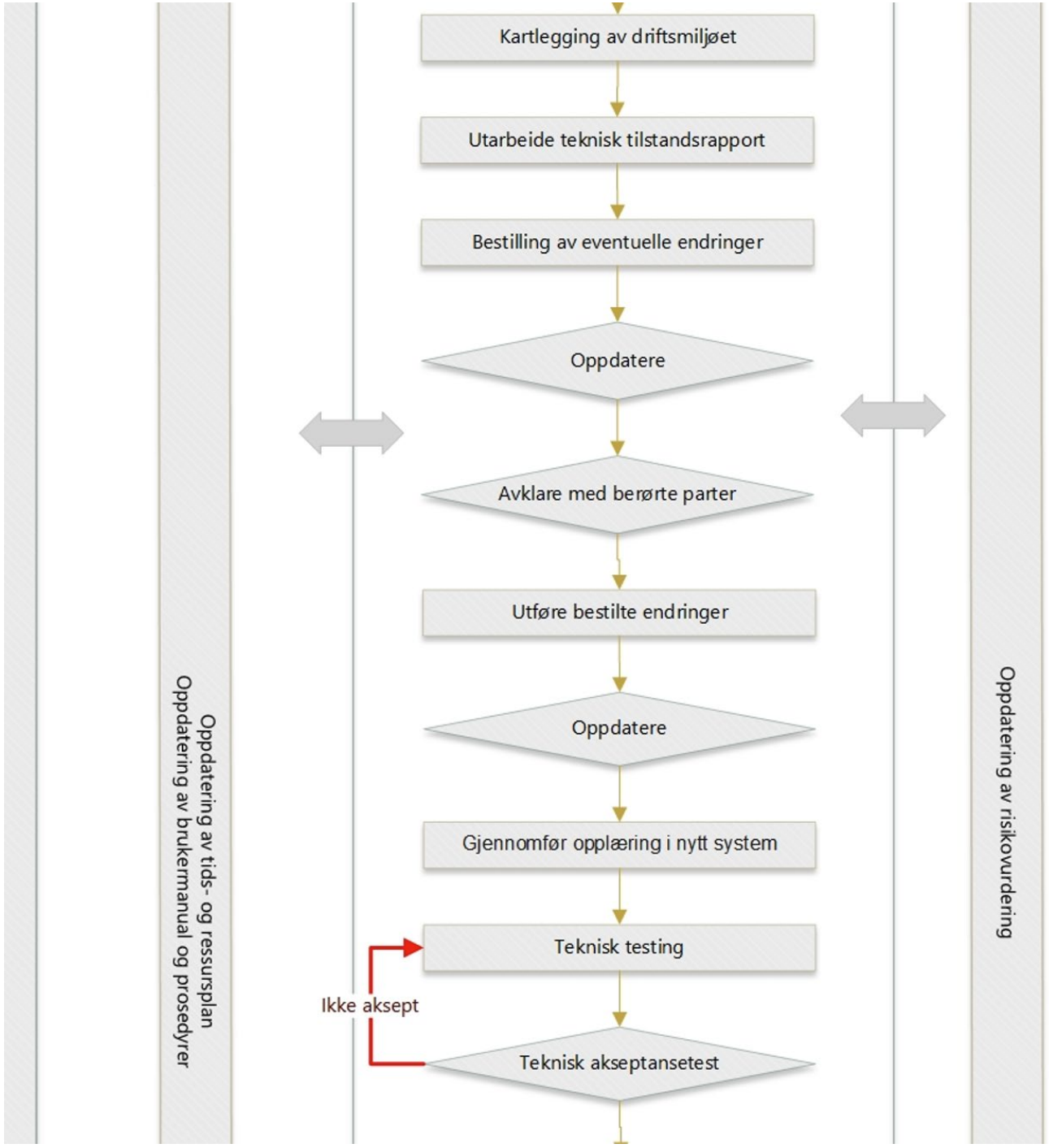
Normens krav i anskaffelser

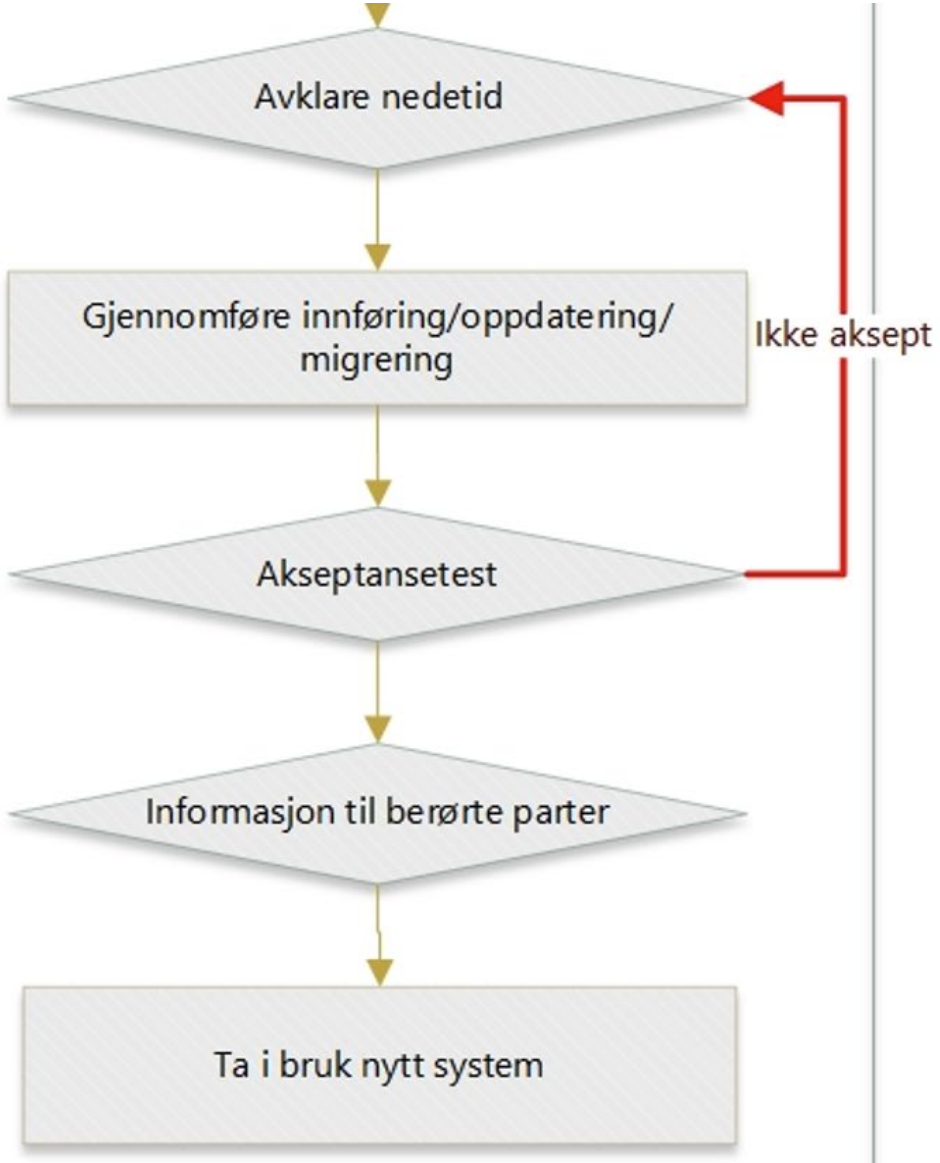
- I anskaffelsesprosesser er det vanlig at det stilles krav til at løsningen skal oppfylle Normen, eller at leverandøren skal følge Normen. Dette kan imidlertid være vanskelig å evaluere for kunden og skape et dårlig grunnlag for en kontrakt. For å kunne evaluere dette på en god måte og danne det beste grunnlaget for kontrakten, er det viktig at både leverandør og kunden har god kommunikasjon og kjennskap til kravene.

Vedlegg

- Flytskjema innføringsprosessen
- HUKI-Matrise


Flytskjema - innføring og oppdatering av systemer
Risikovurdering
Oppstartmøte
Opprett HUKI-Matrise og
avtale mellom kunde og leverandør
Utarbeide tids- og ressursplan
.
Utarbeide testprotokoll, og akseptkriterier.
Avklare med berørte parter


Kartlegging av driftsmiljøet
Utarbeide teknisk tilstandsrapport
Bestilling av eventuelle endringer
Oppdatere
Avklare med berørte parter
Utføre bestilte endringer
Oppdatere
Gjennomfør opplæring i nytt system
Teknisk testing
Ikke aksept
Teknisk akseptansetest
Oppdatering av tids- og ressursplan
Oppdatering av brukermanual og prosedyrer
Oppdatering av risikovurdering


Avklare nedetid
Gjennomføre innføring/oppdatering/ migrering
Ikke aksept
Akseptansetest
Informasjon til berørte parter
Ta i bruk nytt system

HUKI-Matrise

Ansvarsmatrise - HUKI

Matrisen er kun et eksempel. Utfylling av matrisen bør inngå som en del av aktiviteten i oppstartmøte.

H	**H**ovedansvarlig
U	**U**tfører
K	**K**onsulteres
I	**I**nformeres

Nr	Aktivitet / Beslutning	Kunde	Leverandør	Sluttbruker
1	Risikovurdering	H & U	K	K
2	Utarbeide tidsplan			
3	Opprett avtale mellom leverandør og kunde			
	Utarbeide tids- og ressursplan	H & U	K	K
	Utarbeid testprotokoller og akseptkriterier	H & U	K	K
4	Kartlegge driftsmiljøet	U	H	
5	Utarbeide tilstandsrapport på kundens driftsmiljø	H & U	I	
6	Bestilling av eventuelle endringer i infrastruktur og maskinvare	H	I	
7	Teknisk test før man går i produksjon	H	U	K
8	Utføre risikovurdering	H & U	K	K
9	Utarbeide en beskrives hvordan innføring og eventuell konvertering blir gjennomført	I	H & U	K
10	kartlegging av endringer	K	H & U	K
11	Oppdatere brukermanualer	I	H & U	K
12	Oppdatere prosedyrer	H & U	K	K
14	Gjennomfør opplæring i nytt system	I	H & U	I
15	Opprett alle brukere med korrekt rolle og tilgang	U	H	K
16	Arkivering av sikkerhetskopier	H	U	
17	Gjennomgang av konvertering med berørte parter	H	U	K
18	Gjennomføring av konvertering	H	U	
19	Akseptenes av konverterte data	H	K	U
20	Avslutte eksisterende løsninger	H		
21	Utarbeid tester som skal gjennomføres for å kontrollere at konvertering og bytte er gjennomført korrekt	H	I	K
22	Planlegg pasientbehandling uten systemstøtten i den planlagte tiden konvertering og bytte er planlagt	H	K	U
23	Akseptansetest av nytt system	H	K	U
24	Dokumentere akseptansetest	H	U	K
25	Oppdater teknisk dokumentasjon			

Normkonferansen

NOV | 21-22 | 2023

The Qube, Gardermoen

SKANN MEG

Bli med på kurs på Pre-Normkonferansen

Program for Normkonferansen