



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
6.25 (M)	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logger over, jf. Normen kap. 5.4.4: • Autorisert bruk • Alle forsøk på uautorisert bruk <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		
6.26 (M)	Følgende skal minimum registreres i logger, jf. Normen kap.5.4.4.: • Entydig identifikator for den autoriserte brukeren • Hvilke type opplysninger det er gitt tilgang til • Hvilke endringer som er blitt utført («endret fra – endret til») • Hvem som har fått utlevert helseopplysninger som er knyttet til tjenestemottakers eller brukerens navn eller fødselsnummer • Grunnlaget for tilgangen • Tidspunkt og varighet for tilgangen <u>Utformingskrav</u> Leverandøren skriver «Lest og akseptert». Leverandørene viser også hvordan kravet er oppfylt gjennom demonstrasjon iht. oppgitte demosituasjoner i Vedlegg 1 Beskrivelse av demonstrasjoner.	JA
Leverandørens besvarelse: Lest og akseptert		
6.27* (E3)	Løsningen bør ivareta at Kunden kan ta ut en rapport over systembrukere, som viser systembrukers sonetilhørighet, tildelt(e) rolle(r) og tidsperiode for aktiv tilgang. Rapporten kan overføres til excel. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

Handwritten signature/initials.



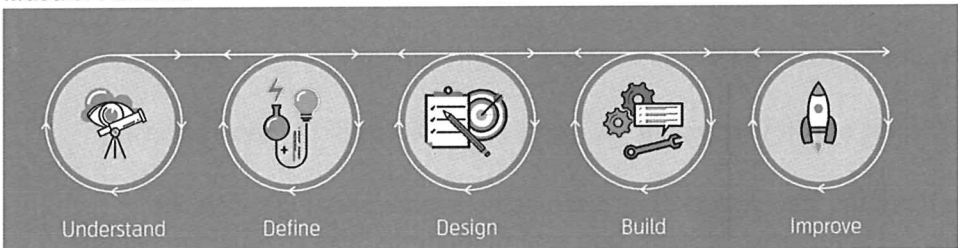
Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Oslo kommunes funksjonskrav er ikke fullstendig implementert i tjenesten for Digitalt tilsyn ved tilbudsinnsending, men vil leveres innenfor angitt frist. Tjenestens administrasjonsløsning har i dag mulighet for å ta ut lister/rapporter på en rekke områder per konto/soneenhet, med relevante opplysninger per rapport, bl.a. rapporter over: • Systembrukere • Tilgangsgrupper • Tjenestemottakere • Roller Rapportene kan eksporteres til Excel. Siste aktive tilgang er pt. tilgjengelig i brukergrensesnitt, ikke inkludert i rapport, men kan kopieres ut fra aktivitetslogg og enkelt filtreres frem i Excel. Ytterligere rapporter og kombinasjonsmuligheter kan utvikles på nærmere spesifikasjon.		
Integritet		
6.28 (M)	Helse- og personopplysninger skal være korrekte og knyttes til rett identifisert person, jf. Normen kap. 3 (integritet). <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenors Digitalt tilsyn tjeneste kan benyttes som en pseudonymisert eller personidentifiserende tjeneste. Enhetene kan også være koblet til lokasjon (adresse/rom) ikke person. Dersom kunden velger å benytte Digitalt tilsyn som en personidentifiserende tjeneste vil alle opplysninger være knyttet til det underliggende tekniske pasient-ressurs i tjenesten. Sikkerhetsløsningen har som beskrevet i krav 6.12, 6.19 og 6.20 mekanismer som verifiserer autorisasjon til å lagre data til aktuell person/ressurs. Løsningen har blitt omfattende testet, både ved intern testing og igjennom uavhengig tredjeparts penetrasjonstest, mtp skrijving av data til feil person, noe som i testene ikke har vært mulig verken igjennom brukergrensesnitt eller forsøk på uautorisert bruk av integrasjonstjenester.		
Innebygget personvern		
6.29 (M)	Løsningens standardinnstillinger skal på forhånd være satt til å være mest mulig personvernvennlig i henhold til Datatilsynets veileder for innebygget personvern eller tilsvarende: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/ <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenors digitalt tilsyn er utformet og utviklet iht prinsippene for innebygget personvern beskrevet i		

Handwritten signature



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	Datatilsynets veileder, denne sammenfaller svært godt med Telenors tjenstedesignprosess. Telenors Digitalt tilsyn er etablert etter denne metodikken som for alle andre tjenester som etableres i Telenor. Tjenstedesignprosessen er basert på iterasjoner, med gjentagende prototyping, utprøving, evaluering og forbedring. Vi legger vekt på tilstrekkelig involvering av relevante brukere og personell, inkludert personvernbeskyrminger og innstillinger, samt involverer Telenors egne personvernspesialister for vurderinger igjennom alle faser av arbeidet. Tjenstedesignprosessen er illustrert under:  Datatilsynets veileder for innebygget personvern og Telenors tjenstedesignprosess sammenfaller som følger (Datatilsynets begreper først, Telenors begreper i parentes). Opplæring (Understand) - alle medarbeidere har gjennomført Telenors obligatoriske opplæringsprogram for personvern. Alle i vårt e-helse tjenesteutviklingsteam har i tillegg spesiell opplæring i personvernakspekter ved tjenesteutvikling. Vi har tilgang på spisskompetanse fra Telenors øvrige personvernfunksjoner og –ombud. En kritisk del av opplæringen er Understand/Innsiktsfasen, hvor vi innhenter mer kunnskap om behov rundt den spesifikke tjenesten, både aktører, arbeidsprosesser, deres kompetanse osv. Krav (Define) - produkter og tjenester etableres med kravstyring, som sikrer at funksjonskrav til løsningen, herunder personvernkrav følges opp igjennom alle faser av prosessen. Både den registrertes rettigheter, virksomhetens plikter og øvrige personvernrelaterte krav spesifisert i helselovgivningen og Normen ivaretas her. Kravstyring er en kontinuerlig prosess som følges opp igjennom alle faser av en produktlivssyklus. Design (Design) - Designfasen gjennomføres basert på gjentatte runder med prototyping, testing og intervjuer med relevante aktører, herunder representative tjenstemottakere, helsepersonell og administratorer. Koding og Test (Build) - Tjenesten er bygget på anerkjente open-source applikasjonsrammeverk med aktive miljøer/communities som bidrar inn i feilretting og forbedring. Koden forvaltes i versjonshåndteringssystemer med automatiserte rutiner for kvalitetssikring. Hver nye kodesnutt gjennomgås av sidemann for uavhengig kvalitetssikring iht utviklingspartners ISO27001 sertifiserte styringssystem og prosedyrer. Tjenesten utvikles i iterasjoner etter smidige prinsipper og test-dreven utviklingsmetodikk. Funksjonalitet, herunder innebygget personvern, testes i små deler underveis, og vi gjennomfører regresjonstest av tidligere etablert funksjonalitet for alle nye hovedversjoner. Produksjonssetting (ikke omhandlet i Telenors tjenstedesignprosess) - Tjenesten digitalt tilsyn gjennomgår Telenors gatekeeperprosess for godkjenning før salg/produksjonssetting. Dette er en	

3/3 *me*



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	kvalitetssikring av alle ledd, fra produktkvalitet til utstyrslogistikk, hendelsesoppfølging, feilretting, support og administrative prosedyrer. Forvaltning (Improve, samt driftsrutiner) - Digitalt tilsyn følger for Telenor e-helse samme prosedyrer som for alle andre velferdsteknologitjenester vi har i drift mtp. Hendeshåndtering, varsling til dataansvarlige mv. For videreutvikling av tjenesten følges tjenstedesignprosessen på nytt dersom større endringer skal gjøres, mens for mindre forbedringer gjennomføres samme prosess i et nedskalert format. Etablert funksjonalitet: Det er flere tekniske mekanismer i tjenesten som bidrar til innebygget personvern: • Kunden kan anvende et fritt valgt antall "kontoer" for høyeste grad av separasjon av informasjon. • Tjenesten kan benyttes uten direkte identifiserende personopplysninger dersom hensiktsmessig, f.eks. ved bruk på institusjon kan romnummer eller pseudonym benyttes istedenfor navn. • Som standard er tilsynsvindu lukket. Administrator må gjøre kamera tilgjengelig for tilsyn for utvalgte tidspunkt før det kan tas i bruk, og tilsynsvinduer kan når som helst begrenses. • Nye operatører har ved registrering ikke tilgang til tjenestemottakers kamera, de må eksplisitt legges til aktuell tilgangsgruppe.	
6.30 (M)	Løsningen skal kun innhente nødvendige personopplysninger iht. det besluttede formålet. Metoder for å begrense mengden personopplysninger kan være: • Særlige kategorier av personopplysninger er utelatt • Fødselsnummer er utelatt • Informasjon som registreres kan kun indirekte identifisere en person (en person vil være indirekte identifiserbar dersom det er mulig å identifisere vedkommende gjennom bakgrunnsopplysninger som f.eks. bostedskommune eller institusjonstilknytning med opplysninger om alder, kjønn, yrke, diagnose eller liknende) • Navn er erstattet med pseudonym <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

AS Helse



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Det er kun et svært begrenset antall personopplysninger som er nødvendig for å benytte tjenesten. Tjenesten kan benyttes uten direkte identifiserende personopplysninger dersom hensiktsmessig, f.eks. ved bruk på institusjon kan romnummer benyttes istedenfor navn. Det kan fritt benyttes pseudonym istedenfor navn. Fødselsnummer er ikke påkrevet med mindre kunden ønsker å benytte dette f.eks. ifbm integrasjon mot Velferdsteknologisk knutepunkt hvor fødselsnummer er påkrevet.		
6.31* (M)	Sletterutiner skal være etablert, og informasjon kan slettes automatisk etter bestemte tidsintervaller, eller når formålet ved behandlingen er opphevet. Dette forutsetter at opplysningene ikke er journalpliktige iht. pasientjournalloven. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt og hvordan dette er dokumentert.	JA
Leverandørens besvarelse: Det er etablert automatiserte sletterutiner for all informasjon som ikke eksplisitt slettes av tjenesteutøver ifbm administrasjon av tjenesten. Registrerte personopplysninger som navn osv. slettes umiddelbart når tjenestemottaker avregistreres fra tjenesten. Telenors vurdering er at tjenesten ikke skal være hovedkilde for journalpliktige opplysninger, dette skal ligge i kommunens EPJ. Shepherd har automatiske sletterutiner for hendelsesloggen i en konto. Ved konfigurasjon av en konto definerer man en TTL (Time To Live) for innslagene i loggen, og de slettes deretter automatisk når de utløper. Det lagres ingen personopplysninger i administrasjonsløsning for personlig gateway. Sletterutiner er følgelig ikke nødvendig. Utstyrskonfigurasjoner (som ikke inneholder personopplysninger) slettes når utstyr slette/avregistreres. Det lagres ingen personopplysninger i administrasjonsløsning for kamera. Sletterutiner er følgelig ikke nødvendig. Utstyrskonfigurasjoner (som ikke inneholder personopplysninger) slettes når utstyr slette/avregistreres.		
6.32 (E3)	Løsningen bør ha muligheter for konfigurering av egendefinerte tidsintervaller for automatisk sletting av spesifikk informasjon. <u>Utformingskrav</u> Leverandøren beskriver hvilke typer data som kan tilknyttes egendefinerte tidsintervaller for sletting. Dette kan f.eks. være data knyttet til: • Tekniske varsler Aktivitetsrelaterte data (bilder, video, lyd, hendelser, varsler, målinger m.m.).	JA

3/11 are



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: Det lagres ingen video, lyd eller andre aktivitetsrelaterte data i løsningen. Det er følgelig ikke heller relevant med sletteintervaller for disse. Hendelser og varsler slettes iht en konfigurerbar TTL (Time To Live) både for hendelser og varsler fra utstyr, og for hendelser og varsler relatert til tjenestemottaker, som beskrevet i svar til kap. 6.31. De mest vanlig brukte sletteintervallene er 30 og 90 dager.		
6.33* (M)	Brukergrensesnittet skal begrense muligheten til å oppgi unødvendig personlig informasjon. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Viktigste tiltak for å forhindre registrering av unødvendig personlig informasjon er at det er svært få felter for registrering av opplysninger i løsningen. Brukergrensesnittet for Telenors digitalt tilsyn er spesielt etablert for formålet med tjenesten og har ingen felter for registrering av unødvendige personopplysninger. Det finnes kun ett generelt fritekstfelt for å angi noe som identifiserer for hvem eller hvor hendelsen har inntruffet, ut over dette er det ingen muligheter for å registrere personopplysninger. I det ene fritekstfeltet som finnes kan en registrere enten fullt navn, eller en adresse, eller et romnummer, eller en annen identifiserende opplysning som et kallenavn, eller et pseudonym etter kommunens ønske.		
6.34 (M)	Lagret informasjon skal være kryptert for å begrense tilgangen til hva for eksempel systemadministrator kan se av personopplysninger. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: All kommunikasjon med systemet, og mellom systemet og eksterne integrasjoner går over krypterte kommunikasjonskanaler. Data som lagres i systemet, både personopplysninger om tjenestemottakere og systembrukere, samt konfigurasjon av tjenesten, lagres kryptert.		
6.35 (M)	Enkelte systembrukere skal kunne sperres for innsyn til enkelte tjenestemottakere, slik at vi kan ivareta innbyggernes rettigheter til å sperre egne helseopplysninger for enkelte ansatte. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA

W. Ape



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
Leverandørens besvarelse: I administrasjonssystem til Shepherd kan administrator for tjenesten konfigurere at en systembruker skal nektes innsyn til en eller flere tjenestemottakere. All tilgang til data for disse tjenestemottakerene vil da bli sperret, uavhengig hvilken rolle brukeren har, og tilgangene som er gitt til rollen.		
6.36 (M)	Det skal være etablert kryptert kommunikasjon over Internett, i databaser og på mobile enheter. Kryptering gjelder alle ledd av verdikjeden som tjenesten består av. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Overordnet arkitekturf figur beskrevet i krav 2.11 viser kommunikasjon mellom ulike komponenter i løsningen. All kommunikasjon i verdikjeden, mellom komponentene nummerert 1-16, har tilstrekkelig kompleks transportkryptering. Noen eksempler: • Axis kamera – Axis Guardian Communication system • Axis Guardian Communication system – Telenor Shepherd • Neat Care Manager – Telenor Shepherd • Telenor Shepherd – ID-porten • Telenor Shepherd – systembrukers klient (pc/nettbrett/mobil) • Neat Care Manager – systembrukers klient (pc/nettbrett/mobil) • Telenor Shepherd – VKP • mv. Med tilstrekkelig kompleks transportkryptering mener Telenor Transport Layer Security (TLS) på standardiserte kommunikasjonsprotokoller som http og websockets. TLS er en Internet Engineering Task Force (IETF) standard som muliggjør ende-til-ende autentisering og privat kommunikasjon ved hjelp av kryptografi. Hvilken krypteringsprotokoll som anvendes i hvert enkelt grensesnitt varierer med hva endepunktene kan støtte, som igjen avhenger av hvilke programvareversjoner som er installert. Telenor har prosedyrer for å sikre oppdatert programvare på alle ledd i verdikjeden som er vårt ansvar, mens kommunen er ansvarlig for å sikre oppdatert programvare på alle ledd i verdikjeden som er kommunens ansvar, for eksempel nettleser på den ansattes pc'er. Dersom ikke programvare er tilstrekkelig oppdatert vil den komponenten med de strengeste sikkerhetskrav avvise kommunikasjon med komponenten med ikke tilstrekkelig sikkerhet, og kommunikasjon kan ikke etableres. Et eksempel på dette er dersom nettleser på kommunens pc kun støtter TLS v1.1 (vurdert per september 2019 som ikke sikker), mens Telenors tjeneste krever TLS v1.2 (nyeste med utbredte standard), eller dersom ikke mest oppdaterte krypteringsalgoritmer benyttes, f.eks ved at en kommunikasjonspart kun støtter RC4 krypteringsalgoritme som er vurdert som usikker for bruk innenfor TLS. Gjeldende sikkerhetsanbefalinger er at grensesnitt er sikret med gyldige sertifikater med minst 2048bits nøkler. Alle grensesnitt i løsningen er sikret med sertifikater med minst 2048bits nøkler		

415 AME



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
utstedt av anerkjent sertifikatmyndighet og gyldighet innenfor aktuell tidsperiode. Telenor har prosedyrer for periodisk fornyelse av sertifikater. Telenor tester komponenter under vårt ansvar bl.a. med SSL-labs. Webserver for Telenors Digitalt tilsyn validerer til karakter A+ (høyeste nivå) per september 2019 (https://www.ssllabs.com/ssltest/analyze.html?d=www.smarttracker.no).		
Håndtering av teknisk sårbarhet		
6.37 (M)	Det skal finnes prosedyrer for å innhente informasjon om tekniske sårbarheter i løsningen. Informasjon innhentes jevnlig, eksponering overfor disse sårbarhetene evalueres og egnede tiltak iverksettes for å håndtere risikoen forbundet med dem. Eksempler på kilder til dette er <u>Microsoft Security TechCenter</u>, <u>Security Bulletins</u>, <u>Cisco Security Advisories and Alerts</u> og <u>Symantec Security Center</u>. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Telenor, partnere og underleverandører har hver sine prosedyrer for kontinuerlig innhenting og evaluering av oppdatert informasjon og trusler og sårbarheter. Kort sammendrag nedenfor: Telenor Norge Security – fortløpende vurdering av generelt trusselbilde og generelle IKT og IoT tekniske sårbarheter basert på en rekke kilder. Anbefaler basert på dette generelle tiltak. Forvalter også Telenor interne IKT- og IoT sikkerhetspolicyer og anbefalte tiltak. Ukentlig intern distribusjon fra Telenor Norge Security og evaluering i Telenor Norge e-helse. Telenor Norge E-helse – Sikkerhetsansvarlig utøver strategi- og internkontrollfunksjon for risikostyring for produktene, bl.a. etterlevelse av Telenor IKT og IoT sikkerhetspolicyer. Sikrer oppfølging av eksternt identifiserte trusler og sårbarheter videre i Telenor Norge e-helse produkter og verdikjede. Produktsjefer holder fortløpende dialog med utstys- og andre underleverandører for oppfølging av endringer i trusler og sårbarheter og evt. endringer av risikovurderinger og tilhørende korrigerende tiltak. Gjelder både brukernært utstyr, programvare og infrastruktur. Ustys- og tjeneste underleverandører utfører fortløpende vurderinger på sine områder. Telenors partnere og underleverandører: Tellu IoT (ISO 27001 sertifisert), Axis Communications (ISO 27001 sertifisert), Neat Electronics (ISO 27001 sertifisert) og AWS (ISO 27001 sertifisert) har alle styringssystemer for informasjonssikkerhet med etablerte prosedyrer for monitorering og oppfølging av risikobildet med trusler og sårbarheter henhold til internasjonal kvalitetsstandard i forhold til aktuelle komponenter, og følger opp relevante sikkerhetsbulletiner og lignende som inkluderer kilder eksemplifisert i kravspesifikasjon og andre som for eksempel blogger, nyhetsbrev, rapporter osv fra Norsis (https://norsis.no/), Nasjonal Sikkerhetsmyndighet (NSM) (https://www.nsm.stat.no/) og Mnemonic (https://www.mnemonic.no/). Utvalg av offentlig publiserte produktspesifikke kilder nedenfor:		

KS HNE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til informasjonssikkerhet	JA/NEI
	- Axis Security Advisory Notification: https://www.axis.com/support/product-security - AWS Security Bulletins: https://aws.amazon.com/security/security-bulletins/ - Kubernetes Security Bulletins: https://cloud.google.com/kubernetes-engine/docs/security-bulletins - Docker Security Blog: https://blog.docker.com/2018/02/secure-supply-chain-kubernetes/ - Android Security Bulletins: https://source.android.com/security/bulletin	
Testmiljø		
6.38 (M)	Det skal tilgjengeliggjøres et testmiljø for applikasjonen som er isolert fra produksjonsmiljøet, der oppgraderinger/nye funksjoner/nye enheter kan testes, før de tilgjengeliggjøres i produksjonsmiljøet. Dette miljøet skal også kunne brukes til utprøving og opplæring av ansatte, med mindre det i tillegg settes opp et eget kursmiljø. Testmiljøet skal kun inneholde fiktive data og må kunne underlegges andre sikkerhetsmekanismer/innstillinger enn produksjonsmiljøet (f.eks. mulighet for å deaktivere to-faktorautentisering og IP-filtrering). Testmiljøet skal være tilgjengelig til teststart hos Kunden. Se <u>Normens faktaark nr. 43</u> Bruk av testdata som inneholder helse- og personopplysninger for ytterligere informasjon. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet oppfylles.	JA
Leverandørens besvarelse: Det vil bli satt opp et testmiljø som kunden kan benytte for akseptansetest samt prøve ut nye sensorer/kamera og teste ny funksjonalitet. Miljøet vil også kunne benyttes ifbm opplæring. Dette miljøet vil driftes som en separat skyløsning, men hvor SLA krav ikke vil være håndhevet. Forutsetter at egnet sted (rom) for test av digitalt utstyr er tilgjengelig hos kunden. Det må finnes en stabil internettlinje tilgjengelig på rom og internettkabel må være på plass til der hvor man ønsker å montere sensor eller kamera. Testmiljøet vil kun inneholde fiktive data og kan underlegges ønskede sikkerhetsmekanismer.		

Tabell 6 – Krav til informasjonssikkerhet

• **Krav til drift og robusthet**

Følgende krav til drift og robusthet skal besvares for alle delkonkurranser.

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til drift og robusthet	JA/NEI
----------	---	--------

AS me



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til drift og robusthet	JA/NEI
7.1 (M)	Drift av løsningen Leverandøren tilbyr en tjenestenivåavtale (SLA) som omfatter: • opptid på minimum 99,9 % på månedlig basis (basert på A og B feil) • tjenesten kan reetableres innen 24 timer dersom datasenter eller system blir utilgjengelig. • økonomisk kompensasjon for brudd på avtalt tjenestenivå • overvåking av løsningen og varsling om avvik fra avtalt tjenestenivå/driftsproblemer/feil til Kunden uten ugrunnet opphold • fortløpende dokumentasjon av tilgjengelighet, innmeldte feil med kritikalitetsnivå og feilrettingstid • daglig sikkerhetskopiering av logger, data og konfigurasjoner • jevnlig rapportering av servicenivå/opptid • rutiner for oppdateringer, vedlikehold og annen planlagt nedetid • definisjonen av A-, B- og C-feil slik den fremgår av SSA-K punkt 2.2.2 • rutiner for håndtering av A, B og C feil (Rapporteringer skjer til sentral forvaltning i Fagsystemavdelingen i Helseetaten) <u>Utformingskrav:</u> Leverandøren dokumenterer sin tjenestenivåavtale (SLA). Denne vil inngå som SSA-K bilag 13.	JA
Leverandørens besvarelse: Leverandøren tilbyr en tjenestenivåavtale (SLA) som skal inntas i Bilag 13. Denne omfatter alle punktene som er gjengitt i kravet: Opptid på minimum 99,9 % på månedlig basis (basert på A og B feil) Ja, dette er inntatt i SLA Tjenesten kan reetableres innen 24 timer dersom datasenter eller system blir utilgjengelig. Ja, dette er inntatt i SLA Økonomisk kompensasjon for brudd på avtalt tjenestenivå Leverandøren tilbyr kompensasjon som er inntatt i SLA Overvåking av løsningen og varsling om avvik fra avtalt tjenestenivå/driftsproblemer/feil til Kunden uten ugrunnet opphold Ja, dette er inntatt i SLA Fortløpende dokumentasjon av tilgjengelighet, innmeldte feil med kritikalitetsnivå og feilrettingstid Ja, prosedyrer for feilhåndtering er beskrevet i SLA Daglig sikkerhetskopiering av logger, data og konfigurasjoner Ja, hver natt, Full backup månedlig til tape, differensiell ukentlig til disk, og inkrementell daglig til		

415
MCE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til drift og robusthet	JA/NEI
	disk. Tape gjenbrukes etter 6 mnd. Jevnlig rapportering av servicenivå/oppetid Ja, leverandøren foreslår at det etableres et samarbeidsforum med Oppdragsgiver hvor partene setter opp en plan for hvordan dette best mulig kan tilpasses partenes behov. Rutiner for oppdateringer, vedlikehold og annen planlagt nedetid Ja, dette er inntatt i SLA. Oppdateringer varsles også til systembruker direkte i brukergrensesnittet. Vedlikehold og annet planlagt vedlikehold på Digitalt Tilsyn og Axis videokamera varsles direkte til systembruker i brukergrensesnittet Definisjonen av A-, B- og C-feil slik den fremgår av SSA-K punkt 2.2.2 Leverandøren har utarbeidet en SLA som inntas i Bilag 13, ref konkurransegrunnlagets bestemmelser. Feilkategoriene A, B og C feil er definert i SSA-K hvor begrepene «utstyr og programvare» benyttes. SSA har også en avtale som heter SSA-L, som er tilpasset en tjenesteleveranse. I SSA-L er «utstyr og programvare» er byttet ut med tjenesten, ellers er de like. Leverandøren leverer en tjeneste, derfor har vi som utgangspunkt valgt å benytte feilkategorisering slik som beskrevet i SSA-L. Rutiner for håndtering av A, B og C feil Ja, prosedyre for håndtering av feil er beskrevet i SLA	
7.2 (E2)	Leverandøren tilbyr en SLA utover minimumskravene i krav 7.1. <u>Utformingskrav:</u> Leverandøren dokumenterer meroppfyllelse i sin tjenestenivåavtale.	JA
	Leverandørens besvarelse: Tjenestenivåavtalen som er lagt ved for å inntas i Bilag 13 inneholder også i tillegg feilrettetider som KPI'er knyttet til feilkategori. Hvis partene avdekker andre KPI'er som på en konstruktiv måte kan tilpasses gjeldene SLA, er Leverandøren åpen for å innta disse for å sikre en trygg tjeneste for Oppdragsgiver.	

Tabell 7 – Krav til drift og robusthet

- Krav til opplæring, bistand og utvikling**

Følgende krav til opplæring, bistand og utvikling skal besvares for alle delkonkurranser.

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
8.1 (M)	Leverandøren skal gi opplæring som er tilpasset ulike roller og funksjoner. Opplæring skal minimum omfatte bruk og konfigurering av enheter og applikasjoner. <u>Utformingskrav</u>	JA

4/5 AM



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

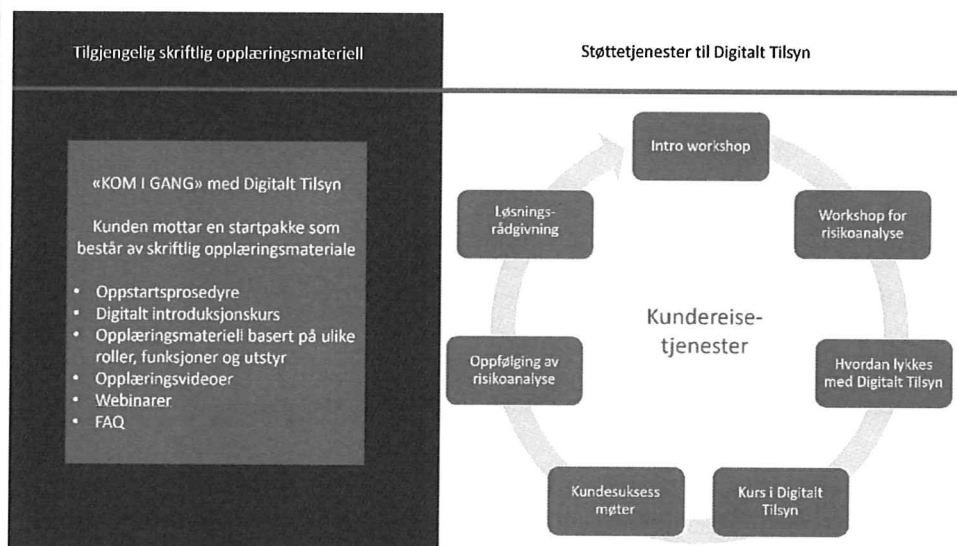
Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
	Leverandøren beskriver hvordan kravet er oppfylt.	

Leverandørens besvarelse:

Vi tilbyr opplæring tilpasset ulike roller og funksjoner.

Figuren under illustrerer både vårt **skriftlige opplæringsmaterie**ll som vil være tilgjengelig for alle som skal ta i bruk våre digitale tilsynsløsninger, samt at vi tilbyr **et sett av kundereise-tjenester** som er ment å støtte kunden i ulike faser ved innføring av Digitalt Tilsyn.

Formålet for begge formene for opplæring er å gi trygghet og mestring i å ta i bruk ny velferdsteknologi.



Det skriftlige opplæringsmaterialet vil være tilgjengelig digitalt og er ment å veilede trinn-for-trinn, hva som skal til for å ta løsningen i bruk. I tillegg tilbyr vi et sett av kundereisetjenester som kunden kan velge fra.

Se nærmere beskrivelse av kundereise-tjenestene:

Intro-workshop (2-4 timers workshop):

En Intro-workshop gir en introduksjon til Digitalt Tilsyn med tanke på hvilke utfordringer tjenesten kan bidra til å løse, hva tjenesten Digitalt Tilsyn fra Telenor består av, en gjennomgang av sikkerhet i løsningene og demonstrasjon av funksjonalitet.

Hvem: Passer i hovedsak for ledelse og administrator som ønsker å komme i gang med en test av Digitalt Tilsyn.

Workshop for risikoanalyse (3 dager)

Vi kan fasilitere en Risk Assessment Workshop i kundens miljø. Dette er en 3 dagers workshop som resulterer i en utbedringsplan som kunden eier. Formålet er å hjelpe kunden å minimere risiko ved

AS
une



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
	introduksjon av digitale tilsynstjenester i deres miljø samt etablere god innsikt i løsning, svake punkter og underlag til kundens egen personvernkonsekvensutredning (DPIA). Hvem: Passer for ledelse, administrator, IT teknikere. “Hvordan lykkes med Digitalt Tilsyn” (5 workshops hos kunden) "Hvordan lykkes med Digitalt Tilsyn" er et sett med workshops som er ment å støtte kunden gjennom digitaliseringsprosjekter for Digitalt Tilsyn og som understøtter Difis anbefalte prosjektmodell "Prosjektveiviseren". Målet er rask og suksessfull adopsjon av digitale tilsynstjenester for å nå investeringsmål og realisere gevinster. "Hvordan lykkes med Digitalt Tilsyn" favner både planlegging, opplæring og evaluering. For pilot og for institusjoner vil vi anbefale gjennomføring av alle tre delene i "Hvordan lykkes med Digitalt Tilsyn". Vi anbefaler alle å gjennomføre "Del 1 – Planlegge for suksess". Del 1 WS 1: Planlegge for suksess Del 2 – Gjennomføre innføring av ny tjeneste WS 2: Kartlegging av nå-situasjon WS 3: Bruker-opplæring WS 4: Jobb smartere Del 3 WS 5: Evaluere og veien videre Hvem: Passer for kunder som skal implementere digitalt tilsyn og som allerede har avklart behov og valgt konsept. De ulike workshopene involverer ulike roller. Se nærmere beskrivelse under punkt 8.4 for gjennomføring av "Hvordan lykkes med Digitalt Tilsyn" workshops. Kurs i Digitalt Tilsyn Vi tilbyr ulike typer kurs i brukeropplæring spesielt rettet mot rollene tjenesteutøver og administrator. Det vil være mulighet for å delta på åpne kurs eller man kan bestille tilpassede kurs i kundens lokaler basert på valgte funksjoner. Hvem: Tilpasset ulike roller hos kunden. Kundesuksess møter Vi tilbyr månedlig statusmøter hvor vi gjennomgår status på digitale tilsynstjenester, gjennomgår utfordringer og lager utbedringsplaner for disse, samt gjennomgår nyheter og endringer i tjenesten. Hvem: Passer for ledelse og administrator.	

Handwritten signature



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
8.2 (E2)	Leverandøren bør ha et opplæringsopplegg som er godt tilpasset de ulike rollene i løsningen. <u>Utformingskrav</u> Beskriv hvilke roller/funksjoner det foreslås å tilpasse opplæring for, og hvordan innhold og struktur i kurset kan legges opp. Beskriv også eventuelle muligheter for e-læring.	JA
Leverandørens besvarelse: For å ta i bruk Digitalt tilsyn fra Telenor tilbyr vi ulike moduler som kunden kan velge fra. Modulene er etablert med utgangspunkt i Kundereise-tjenester som beskrevet i punkt 8.1 som er et sett av tjenester som vil hjelpe kunden å lykkes med å ta i bruk ny velferdsteknologi. For institusjoner anbefaler vi å gjennomføre alle 5 workshops i "Hvordan lykkes med Digitalt Tilsyn" • WS 1: Planlegge for suksess (oppstartsmøte) • WS 2: Kartlegging av nå-situasjon • WS 3: Brukeropplæring • WS 4: Jobb smartere • WS 5: Evaluere og veien videre For mindre enheter anbefaler vi minimum å gjennomføre WS 1 (Planlegge for suksess) samt deltakelse på kurs tilpasset rolle og funksjon. Vi tilbyr opplæring rettet mot: • Ledelse og administrasjon - hvor vi har fokus på å definere klare mål for innføring av ny teknologi, hva som skal til for å lykkes med innføring av Digitalt Tilsyn og hvordan identifisere og planlegge realisering av gevinster • Administrator – hvor vi vektlegger bruk og konfigurasjon av enheter og applikasjoner, feilsøking og supportrutiner • Tekniker – hvor vi fokuserer på hvilke tekniske forutsetninger som skal til for å skape best brukeropplevelse og gevinstrealisering • Tjenesteutøver – hvor vi fokuserer på trygghet i å ta i bruk tjenesten (brukeropplæring) og hvordan smart bruk av tjenesten kan forbedre arbeidshverdagen • Pårørende – vi bistår med informasjon og opplæringsmateriell til pårørende Vellykkede endringer skjer sjelden av seg selv og vi mennesker er ofte skeptiske til det som er nytt. Innføring av nye tjenester handler vel så mye om å skape motivasjon for endring. Vi tror at ved å sette mennesket i sentrum for opplæringen og ikke teknologien i seg selv, så vil man se egen nytte av å ta i bruk den nye tjenesten, skape et ønske om å ta den i bruk, samt inspirere andre til å dra nytte av fordelene med ny velferdsteknologi. For alle de ulike rollene og funksjonene legger vi vekt på å formidle: • Hvorfor noe skal gjøres annerledes? (Fokus på målbildet) • Hva skal endres? (nå vs framtid)		

AS
GAC



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
- Hvem skal ta del i endringen? - Hvordan påvirker endringen meg?		
8.3 (E2)	Leverandøren bør tilby gode brukerveiledninger og tilgang til veiledningsmateriale som sikrer «hjelp-til-selvhelp» for ansatte i utførende tjeneste. Materialet bør bidra til at ansatte på stedet (hos tjenestemottaker), kan få hjelp og friske opp kompetanse fra kurs når de står fast. <u>Utformingskrav</u> Beskriv hvordan ansatte kan få «hjelp-til-selvhelp» i sin arbeidshverdag. Beskriv f.eks. tilgang på instruksjonsvideoer eller annen e-læring «on-the-spot».	JA
Leverandørens besvarelse: Vi tilbyr et sett med skriftlig opplæringsmaterieell som er ment å sikre “hjelp-til-selvhelp”. Her vil det finnes opplæringsmaterieell i form av: - Digitalt introduksjonskurs - Opplæringsmaterieell (brukerveiledninger) basert på ulike roller, funksjoner og utstyr - Opplæringsvideoer - Webinarer - FAQ Brukerveiledningene beskriver med tekst og illustrasjoner hvordan de ulike rollene går fram for å utføre de handlinger som kreves av dem i applikasjonen. Brukerveiledninger holdes kontinuerlig oppdatert og kan nås til enhver tid. Det tilbys jevnlig webinarer som kundene kan melde seg på, hvor leverandøren gjennomgår digitale tilsyns-tjenester. Temaene varierer og er ment å hjelpe kundene å bruke våre digitale tilsynstjenester på en smart og effektiv måte. Hvis kunden ikke får deltatt på selve webinarer, kan de se opptak av webinarer i etterkant når det passer dem. Det finnes en guide (FAQ – Frequently Asked Questions) hvor brukerne kan få tips til kjente spørsmål som andre har spurt om tidligere.		
8.4 (M)	Leverandøren skal ha en realistisk og gjennomførbar plan for opplæring. Leverandøren skal utarbeide en plan for gjennomføring av opplæring iht. plan i Bilag 4. Planen skal godkjennes av Kunden. <u>Utformingskrav</u> Beskriv hvordan et opplæringsløp kan gjennomføres.	JA
Leverandørens besvarelse: Opplæring handler vel som mye om å forberede de som blir berørt av den nye tjenesten på endringen		

AS Moe

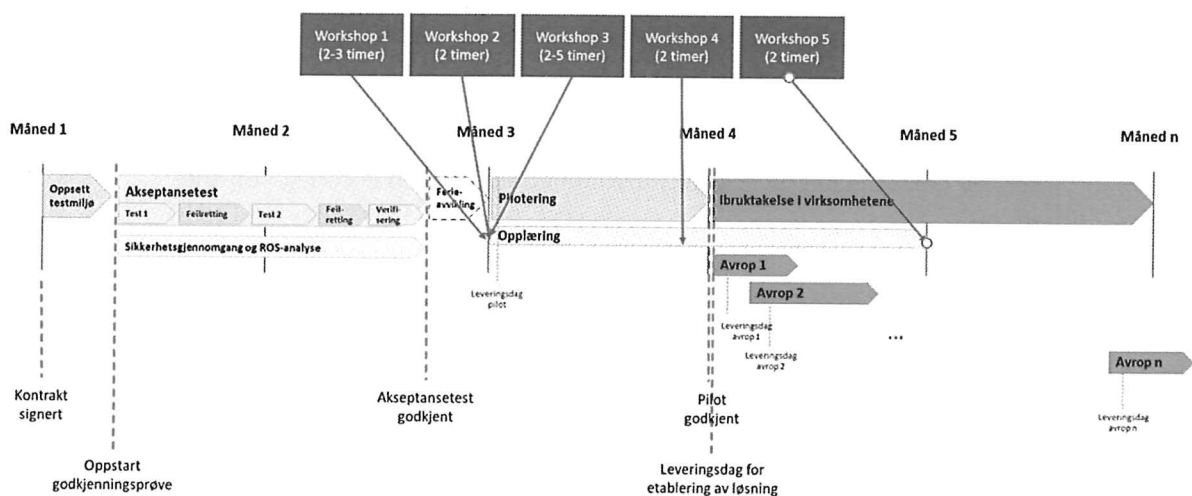


Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
----------	--	--------

som kommer, som å ta i bruk selve tjenesten. Vi anbefaler derfor å gjennomføre kundereise-tjenesten "Hvordan lykkes med Digitalt Tilsyn" som utgangspunkt for opplæringen.

"Hvordan lykkes med Digitalt Tilsyn" består av 5 workshops som er delt i 3 faser.



Del 1, "Planlegge for suksess" (workshop 1), handler om å definere en klar målsetning, planlegge gevinster og hvordan de skal måles, formulere verdibudskap for de ulike parter som blir involvert, legge en realistisk suksessplan for involverte parter (hvem gjør hva), kartlegge hindringer tidlig i prosessen og iverksette tiltak for å lykkes med innføring av ny teknologi. Del 1 passer for ledelse og administrator og gjennomføres før oppstart av pilot.

Del 2, "Gjennomføre innføring av ny tjeneste" består av 3 workshops.

- **"Kartlegging av nå-situasjon"** (workshop 2): Denne workshopen handler om å kartlegge nå-situasjon og forberede ny situasjon noe som både bidrar til å kunne måle gevinster samt tilpasse opplæringen til kundens hverdag. Den utføres i form av intervjuer med tjenesteutøvere og ledelse og gjennomføres før oppstart av pilot.
- **"Brukeropplæring"** (workshop 3): Denne workshopen handler om brukeropplæring og setter mennesket i fokus. Den gjennomføres før pilot-fasen. Med de ulike rollene gjennomgår vi hvorfor noe skal gjøres annerledes (med fokus på kundens målilde), hva endringen går ut på (nå-situasjon versus framtidig situasjon), hvem som blir berørt av endringen og hvordan endringen påvirker den enkelte. Deretter gjør vi scenariobasert opplæring hvor vi gjennomgår funksjonalitet i tjenesten og hvordan de ulike rollene benytter applikasjon og utstyr til å utføre sine arbeidsoppgaver.
Basert på kartlegging av kundens hverdag forsøker vi å gjøre opplæringen så reell som mulig slik at de kjenner seg igjen i utfordringer de opplever i eksisterende jobbhverdag. Vi vil også gjøre noen beredskapsøvelser for å trene på at noe uforutsett skjer og reflektere over hvordan slike situasjoner bør håndteres. Deltakere vil få informasjon om hvor de videre kan finne hjelpe

AS Ace



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI
til selv-hjelp og hvordan de via kundens administrator kan melde inn supportsaker. • “Jobb smartere” (workshop 4): Den fjerde workshopen handler om justering av digitale tilsynsløsninger og arbeidsprosesser som hjelper kunden å jobbe smartere. Workshopen gjennomføres ved slutten av pilot-fasen for å samle erfaringer og kunne gjøre justeringer før man går inn i fasen “Ibruktakelse i virksomhetene”. Del 2 involverer både ledelse, tjenesteutøvere, administrator og evt andre som blir berørt av tjenesten f.eks teknikere, pårørende etc. Del 3, “Evaluere og veien videre” (workshop 5) er en workshop hvor vi etter 1 måned med ibruktakelse, ser på resultat fra oppdatert brukerundersøkelse og målinger samt kartlegger erfaringer. Deretter legger vi en plan for hvordan jobbe smart videre med digitalt tilsyn. Del 3 passer for ledelse og administratorer. Merk: Hvis man ønsker en enklere form for opplæring, kan kunden be om “tilpasset opplæring hvor vi tar utgangspunkt i innholdet i workshop 3 beskrevet over.		
8.5 (M)	Leverandøren skal oppdatere Kunden skriftlig om endringer i produkt/løsning fortløpende, gjennom f.eks. releasenotes ved hver nye versjon/ending. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA
Leverandørens besvarelse: Systembrukere av Digitalt Tilsyn vil motta nyhetsvarsel direkte i applikasjonen om ny funksjonalitet og endringer. Releasenotes er også tilgjengelig på web. Planlagt vedlikehold vil varsles direkte i applikasjonen for systembrukere for å sikre at denne type informasjon når sluttbrukerne.		
8.6 (M)	Leverandøren skal tilby feilretting 24/7/365 for kritiske feil (A-feil) i henhold til definisjon i SSA-K pkt. 2.2.2 for å innfri krav 7.1. <u>Utformingskrav</u> Leverandøren beskriver hvordan feilretting kan tilbys når løsningen er i drift.	JA
Leverandørens besvarelse: Feilretting og prosedyrer knyttet til dette er beskrevet i SLA som inntas i Bilag 13. Det er inntatt en tabell i SLA som viser forventet respons- og feilrettetider for ulike feilkategorier. Det er i tillegg beskrevet en eskaleringsprosedyre.		

4/5 Ace



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI						
8.7 (M)	Leverandøren skal tilby teknisk og funksjonell support mellom kl. 08:00 – 16:00 på hverdager. Det gjøres oppmerksom på at Kunden har en sentral forvaltning i Helseetaten. Denne forvaltningsorganisasjonen vil ofte fungere som førstelinje-support for virksomhetene. <u>Utformingskrav</u> Leverandøren beskriver hvordan support kan tilbys når løsningen er i drift.	JA						
Leverandørens besvarelse: Telenor har dedikert support for velferdsteknologi hvor henvendelser håndteres av personell med kompetanse på Telenors velferdsteknologiske produkter. 08:00 – 16:00 er Telenor tilgjengelig på dedikert telefonnummer. Skriftlige henvendelser behandles også til dedikert epost adresse. Hvis det benyttes epost for å åpne en sak hos Telenor vil kunden automatisk få tilbake et unikt saksnummer fra vårt system. Telenors support avdeling jobber tett med innsender på alle henvendelser slik at eventuell nedetid eller tid uten full funksjonalitet kan reduseres så mye som mulig. Telenor benytter standardiserte metoder for feilsøking og feilretting. Telenors support team involverer ved behov Tellu support for å sikre at riktig kompetanse benyttes til å løse supportsaker.								
8.8 (M)	Opsjon: Leverandør tilbyr teknisk og funksjonelle support utover kl. 08:00-16:00. Det gjøres oppmerksom på at Kunden har en sentral forvaltning i Helseetaten. Denne forvaltningsorganisasjonen vil ofte fungere som førstelinje-support for virksomhetene. <u>Utformingskrav</u> Leverandøren beskriver hvordan support kan tilbys når løsningen er i drift, og priser følgende bistandsnivåer i SSA-K bilag 7: • Support kl. 16:00-22:30 på hverdager • Support helg og helligdager kl. 09:00-22:30 • Support 24/7/365 Pris på opsjonene evalueres ikke. Det bemerkes at priser på opsjoner vil være avgjørende for hvorvidt oppdragsgiver utløser opsjoner eller ikke.	JA						
Leverandørens besvarelse: Vi kan tilby utvidet support basert på følgende vilkår: <table><tr><th>Utvidet support</th><th>Pris per måned</th></tr><tr><td>Support kl. 16:00-22:30 på hverdager</td><td>NOK 318.000 pr måned. Prisen inkluderer inntil 100 supporthenvendelser per måned.</td></tr><tr><td>Support helg og helligdager kl. 09:00-</td><td>NOK 318.000 pr måned.</td></tr></table>			Utvidet support	Pris per måned	Support kl. 16:00-22:30 på hverdager	NOK 318.000 pr måned. Prisen inkluderer inntil 100 supporthenvendelser per måned.	Support helg og helligdager kl. 09:00-	NOK 318.000 pr måned.
Utvidet support	Pris per måned							
Support kl. 16:00-22:30 på hverdager	NOK 318.000 pr måned. Prisen inkluderer inntil 100 supporthenvendelser per måned.							
Support helg og helligdager kl. 09:00-	NOK 318.000 pr måned.							

Handwritten signature



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI																
22:30	Prisen inkluderer inntil 100 supporthenvelser per måned.																	
Support 24/7/365	NOK 318.000 pr måned. Prisen inkluderer inntil 100 supporthenvelser per måned.																	
Tilbudet inkluderer inntil 100 supporthenvelser per måned. For supporthenvelser utover dette volumet vil det beregnes en timepris på NOK 1530 per påbegynte time. Eksempelvis innebærer dette at en support-henvendelse som medfører 1 time og 40 minutter arbeid for Leverandør, så vil det beregnes og faktureres for 2 timers arbeid. Dersom Utvidet support anskaffes på mer enn en delkonkurranse, så gis det 50% avslag i den faste månedsprisen på hovedfunksjon nummer 2 og 65% avslag i den faste månedsprisen på hovedfunksjon nummer 3. Som eksempel; hvis Oppdragsgiver anskaffer 2 hovedfunksjoner fra Leverandør vil den faste månedsprisen (som inkluderer 100 supporthenvelser) på hovedfunksjon 1 være 318.000, mens tilsvarende månedspris for hovedfunksjon 2 (som også inkluderer 100 supporthenvelser) vil være NOK 159.000. Følgende tabell oppsummerer tilbudet: <table border="1"><thead><tr><th>Antall delkonkurranser fra Telenor</th><th>Pris per måned</th><th>Ant. support-henvendelser inkludert per måned</th><th>Pris per påbegynte time utover det inkluderte ant. supporthenvelser i månedspris</th></tr></thead><tbody><tr><td>1</td><td>318.000</td><td>100</td><td>NOK 1530</td></tr><tr><td>2</td><td>477.000</td><td>200</td><td>NOK 1530</td></tr><tr><td>3</td><td>588.300</td><td>300</td><td>NOK 1530</td></tr></tbody></table>			Antall delkonkurranser fra Telenor	Pris per måned	Ant. support-henvendelser inkludert per måned	Pris per påbegynte time utover det inkluderte ant. supporthenvelser i månedspris	1	318.000	100	NOK 1530	2	477.000	200	NOK 1530	3	588.300	300	NOK 1530
Antall delkonkurranser fra Telenor	Pris per måned	Ant. support-henvendelser inkludert per måned	Pris per påbegynte time utover det inkluderte ant. supporthenvelser i månedspris															
1	318.000	100	NOK 1530															
2	477.000	200	NOK 1530															
3	588.300	300	NOK 1530															
8.9 (M)	Leverandør skal ha en dedikert kundeansvarlig som er ansvarlig for Leverandørens leveranser. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivaretatt.	JA																
Leverandørens besvarelse: Dedikert kundeteam for Oslo kommune Telenor har en dedikert kundeansvarlig for våre leveranser til kunden gjennom hele leveranseløpet. I tillegg til Telenors support for velferdsteknologi er det dedikert et kundeteam for leveransene til Oslo																		

Handwritten signature



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI												
kommune: Oslo Kommune er en stor og strategisk viktig kunde for Telenor. Telenors Kundeteam vil lede betjeningen av Oslo kommune og tilhørende virksomheter. Telenors support for velferdsteknologi vil være det daglige kontaktpunktet for bestillinger, leveranser og feilhåndtering. Telenors Kundeteam ledes av Key Account Manager (KAM) som har det overordnede ansvaret for kontrakten med Oslo Kommune. I tillegg vil kundeteamet ha medarbeidere med kompetanse på tjenester og løsninger som leveres under avtalen. Contract Manager (CM) og produksjef for Digitalt tilsyn er sentrale medlemmer i teamet og løsningsekspertene fra hhvs Telenor og Tellu vil delta i teamet ved behov (jmf pkt 8.10). I vår betjeningsmodell legger vi vekt på å skape kvalitet og merverdi gjennom videreutvikling av tjenester som skaper verdi for Oslo kommune. Tett samarbeid mellom partene er en viktig suksessfaktor. Kundeteamet ivaretar kundeutvikling og driftsoppfølging via flere møtearenaer, hvor ledermøter er en naturlig del av samarbeidet. Kundeteamet har ulike ansvarsområder: • Ett kontaktpunkt • Én kontraktforvalter i avtaleperioden • Rapporter • Oversikt over eksisterende løsning og tjenester Kundeteamet for Oslo kommune/Digitalt Tilsyn i Telenor består av: <table><tr><td>Anne Lene Schartum</td><td>KAM Kundeansvarlig</td><td>Tlf. nr. 479 00 202 Mail: anne-lene.schartum@telenor.com</td></tr><tr><td>John-Smith.Kristiansen</td><td>Rolle Contract Manager</td><td>Tlf. nr. 412 45 968 Mail: John-Smith.Kristiansen@telenor.com</td></tr><tr><td>Lars Bakken</td><td>Rolle Leder E-helse</td><td>Tlf. nr. 479 01 901 Mail: Lars.Bakken@telenor.com</td></tr><tr><td>Caroline Cappelen</td><td>Rolle Prod.sjef Digitalt tilsyn</td><td>Tlf. nr. 995 09 108 Mail: caroline.cappelen@telenor.com</td></tr></table>			Anne Lene Schartum	KAM Kundeansvarlig	Tlf. nr. 479 00 202 Mail: anne-lene.schartum@telenor.com	John-Smith.Kristiansen	Rolle Contract Manager	Tlf. nr. 412 45 968 Mail: John-Smith.Kristiansen@telenor.com	Lars Bakken	Rolle Leder E-helse	Tlf. nr. 479 01 901 Mail: Lars.Bakken@telenor.com	Caroline Cappelen	Rolle Prod.sjef Digitalt tilsyn	Tlf. nr. 995 09 108 Mail: caroline.cappelen@telenor.com
Anne Lene Schartum	KAM Kundeansvarlig	Tlf. nr. 479 00 202 Mail: anne-lene.schartum@telenor.com												
John-Smith.Kristiansen	Rolle Contract Manager	Tlf. nr. 412 45 968 Mail: John-Smith.Kristiansen@telenor.com												
Lars Bakken	Rolle Leder E-helse	Tlf. nr. 479 01 901 Mail: Lars.Bakken@telenor.com												
Caroline Cappelen	Rolle Prod.sjef Digitalt tilsyn	Tlf. nr. 995 09 108 Mail: caroline.cappelen@telenor.com												
8.10 (M)	Leverandøren skal etter forespørsel fra Kunden stille en ressursperson til disposisjon i forbindelse med testing, integrasjon og utvikling. <u>Utformingskrav</u> Leverandøren beskriver hvordan kravet blir ivarettatt.	JA												

AS are



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til opplæring, bistand og utvikling	JA/NEI																																																						
Leverandørens besvarelse: Vi vil i forbindelse med testing, integrasjon og utvikling kunne stille relevante ressurser til disposisjon for kunden. Telenor besitter sammen med vår samarbeidspartner Tellu, tverrfaglig sammensatt og svært bred kompetanse på velferdsteknologiske løsninger. Vi tror at et av suksesskriteriene for å realisere gevinster med bruk av ny teknologi i helsetjenesten er knyttet til møtet mellom utvikleren og helsepersonellet som sammen finner gode løsninger på hvordan behov kan dekkes. Videre er det en forutsetning at vi har spisskompetanse på områder som test, sikkerhet, personvern, design, drift og support for å sikre en robust verdikjede for de ulike produktene som leveres. For nærmere informasjon om hvilken kompetanse våre team besitter viser vi til kompetansematrisen fra kvalifikasjonsgrunnlaget.																																																								
 Kompetansematrise <table><tr><th>Faglige kvalifikasjoner</th><th>Prosjektlederkompetanse</th><th>Konseptutvikling</th><th>Funksjonell arkitektur</th><th>Løsningsskisse</th><th>Sikkerhetsarkitektur</th><th>Utviklerkompetanse</th><th>Integrasjonsutvikling</th><th>Endringsledelse</th><th>Gevinstanalyse</th><th>GDPR/personvern</th><th>Informasjonssikkerhet</th><th>Riskostyring</th><th>Brukertesting</th><th>Interaksjons design</th><th>Universell utforming</th><th>Testledelse/testing</th><th>Inføringskompetanse</th><th>Drift & support</th><th>Kundesupport</th><th>Felleskap/felireting</th><th>Applikasjonsforvaltning</th><th>Nettverkskompetanse</th><th>Helsefag/medisin</th><th>Velferdsteknologi</th><th>Nasjonale e-helseløsninger</th><th>Utdanning</th></tr><tr><th>Navn</th><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>			Faglige kvalifikasjoner	Prosjektlederkompetanse	Konseptutvikling	Funksjonell arkitektur	Løsningsskisse	Sikkerhetsarkitektur	Utviklerkompetanse	Integrasjonsutvikling	Endringsledelse	Gevinstanalyse	GDPR/personvern	Informasjonssikkerhet	Riskostyring	Brukertesting	Interaksjons design	Universell utforming	Testledelse/testing	Inføringskompetanse	Drift & support	Kundesupport	Felleskap/felireting	Applikasjonsforvaltning	Nettverkskompetanse	Helsefag/medisin	Velferdsteknologi	Nasjonale e-helseløsninger	Utdanning	Navn																										
Faglige kvalifikasjoner	Prosjektlederkompetanse	Konseptutvikling	Funksjonell arkitektur	Løsningsskisse	Sikkerhetsarkitektur	Utviklerkompetanse	Integrasjonsutvikling	Endringsledelse	Gevinstanalyse	GDPR/personvern	Informasjonssikkerhet	Riskostyring	Brukertesting	Interaksjons design	Universell utforming	Testledelse/testing	Inføringskompetanse	Drift & support	Kundesupport	Felleskap/felireting	Applikasjonsforvaltning	Nettverkskompetanse	Helsefag/medisin	Velferdsteknologi	Nasjonale e-helseløsninger	Utdanning																														
Navn																																																								

Tabell 8 – Krav til opplæring, bistand og utvikling

- Krav til plan og metode for gjennomføring**

Følgende krav til plan og metode for gjennomføring skal besvares for alle delkonkurranser.

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI
9.1 (E3)	Fra kontraktsgenerering til driftsstart (fram til ibruktakelse i virksomhetene): Leverandørs plan og metode for gjennomføring av det aktuelle oppdraget bør være realistisk i forhold til Kundens utkast til fremdriftsplan (se Bilag 4 – «Leveringstidspunkt og andre frister»). <u>Utformingskrav</u> Leverandøren beskriver sin tilnærming til hvordan oppdraget kan	JA

AS Arc



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI
	gjennomføres. Beskriv aktuelle aktiviteter, ansvarsfordeling og tidsestimater, og hva Kunden må legge til rette for/stille med av ressurser for at planen skal kunne gjennomføres (inkl. tidsestimat for Kundens ressursbruk).	
Leverandørens besvarelse: Med utgangspunkt i kundens utkast til fremdriftsplan samt Telenors modell for innføring av Digitalt tilsyn har vi utarbeidet et forslag til aktivitetsplan: MP1- kontraktssignering og oppstartsmøte (Kunde/Leverandør) Ved kontraktssignering avtales det umiddelbart et oppstartsmøte. Oppstartsmøtet vil dekke områder som kommunikasjonsstrategi, plan for akseptansetest, testmiljø, tekniske forutsetninger, testcase, opplæring av testleder/testere samt påbegynne dialog om opplæring og pilotering. Kunden må forberede overnevnte punkter samt stille med relevante ressurser i møtet (2 timer). MP2 - oppsett av testmiljø (Leverandør/Kunde, MP1 + 14 dager) Forutsetter at egnet sted (rom) for test av digitalt utstyr er tilgjengelig hos kunden. Det må finnes en stabil internettlinje tilgjengelig på rom og internettkabel må være på plass der hvor man ønsker å montere sensor/kamera. Dette miljøet kan også brukes til utprøving og opplæring av ansatte. Når forutsetningene over er på plass må kunden beregne ca 1 time pr hovedfunksjon. MP3 -Opplæringsplan godkjent av kunden (Leverandør, MP2 + 20 dager) Leverandør oversender forslag til opplæringsplan basert på innspill fra kunden i oppstartsmøte. Opplæringsplan gjennomgås før godkjenning. I samme møte drøftes videre plan for pilotering etter endt akseptansetest; kundebehov /pains, omfang, lokasjon, forutsetninger for oppstart/installasjon og leveranser for øvrig. Leverandør utarbeider også sjekkliste for pilotering. Kunden må forberede overnevnte punkter samt stille med relevante ressurser i møtet (2 timer). MP4 -Akseptansetest godkjent (Kunde/Leverandør, MP2 + 50 dager) Akseptansetest utføres basert på testcase ihht leverandørens besvarelse. Funn kommuniseres som avtalt i kommunikasjonsplan. I forkant oversender leverandør testlogg fra leverandørens testing til kunden som beskriver antall feil og kategorisering av disse. Akseptansetest godkjennes og løsning er klar for pilotering som neste ledd før endelig godkjenning (jmf Bilag 5 Godkjenningsprøven). Vi estimerer 3 timer pr hovedfunksjon pr iterasjon og anbefaler at det settes av inntil 2 uker for hele testgjennomføringen. MP5- Opplæring i bydelene påbegynt (Kunde/Leverandør, MP2 + 50 dager) Opplæringslengde avhenger av valgt type opplæring (ref punkt 8.4) som tilpasses kundens behov og ønsker. For pilot anbefaler vi kundereise-tjenesten «Hvordan lykkes med Digitalt Tilsyn». Estimerer for kundens ressursbruk: 11 timer pr deltaker. Dette kan justeres ned og tilpasses kundens ønsker. MP6 -Sikkerhetsgjennomgang fullført (kunde/leverandør, MP2 + 50 dager) Leverandør kan bistå med å fasilitere en Workshop for Risikoanalyse i kundens miljø jmf krav 8.1.		

AS Ave



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI
Estimater for kundens ressursbruk: deltakelse fra relevante interne ressurser, herunder virksomhetsansvarlig, sikkerhetsleder, personvernrådgiver, tjenesteutøver med kjennskap til tjenesteutøvelsen i praksis. 2 timer forberedelser samt 8 timer deltakelse på ws pr person. Alternativt til en fullstendig workshop for risikoanalyse i regi av leverandør kan Telenor bidra med relevant kompetanse i kundens egen risikoworkshop, herunder kompetanse på sikkerhetsvurderinger, personvern, kompetanse på løsningen som helhet. MP7 -Rapport sikkerhetsgjennomgang med plan for evt utbedring av leverandøren (Kunde, MP6 + 20 dager) Leverandøren mottar dokumentasjon fra kunde på eventuelle utbedringsområder. Rapporten drøftes i eget møte for å sikre felles forståelse. MP8 -Leverandøren har utbedret eventuelle avvik funnet i sikkerhetsrevisjonen (Leverandør, MP7 +14 dager) Leverandøren formidler status til kunden på utbedring av sikkerhetsrisiki som leverandøren er ansvarlig for, så snart dette er gjennomført og senest 14 dager etter mottatt rapport. MP9 -Leveringsdag for etablering av løsning (MP7 + 14 dager) Løsningen er nå klar for siste del av godkjenningsprosessen; pilotering med utvalgte sykehjem/bydeler.		
9.2 (M)	Godkjenningsprøve Før løsningen aksepteres for drift skal det gjennomføres en godkjenningsprøve. Art og omfang av denne prøven er beskrevet i «SSA-K Bilag 5 – Godkjenningsprøve», ref. SSA-K punkt 2.2.2. <u>Utformingskrav</u> Leverandøren beskriver sin tilnærming til hvordan oppdraget kan gjennomføres. Beskriv aktuelle aktiviteter, ansvarsfordeling og tidsestimater, og hva Kunden må legge til rette for/stille med av ressurser for at planen skal kunne gjennomføres (inkl. tidsestimat for Kundens ressursbruk).	JA
Leverandørens besvarelse: 1.Akseptansetest: Planlegging gjennomføres i oppstartsmøte (MP1). Testene ledes og gjennomføres av kunden i deres lokaler. Leverandøren har i forkant etablert testmiljø for dette formål og selve testgjennomføringen baseres på kundens egne testcase. Formålet er å revidere etterlevelse av kravene ihht Leverandørens besvarelse mtp funksjonalitet, brukervennlighet, ytelse samt personvern og informasjonssikkerhet. I tillegg til ressurser fra kunden stiller leverandøren med nøkkelpersonell tilgjengelig for å understøtte akseptansetestprosessen der det er behov for det. I forkant av selve testgjennomføringen anbefaler vi at testleder og testere deltar på Intro-workshop a 2 timer for å bygge kompetanse på løsning. <u>Forutsetninger:</u>		

AS ARE



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI
	• Testmiljø er etablert og sensorer og kamera er montert ○ Kunden må stille disponibelt lokale samt nødvendige tekniske ressurser for å bistå. Leverandøren besørger øvrig aktiviteter og kostnader for å etablere testmiljø. • Tilgjengelig nettverk samt nødvendige nettverksporter er åpnet ○ Kunden må påse at nettverk er tilgjengelig og nettverksporter er åpnet, etter anvisning fra leverandøren • Kunden har etablert testplan og testcase • Testleder/testere har deltatt på intro-workshop ○ Kunden utpeker og frigjør relevante ressurser, leverandøren foreslår tidspunkt og gjennomfører opplæring Testgjennomføring for totalt 3 delkonkurranser: 3 timer pr hovedfunksjon, samt 1-2 iterasjoner med feilretting og retest. Vi anbefaler at det settes av totalt 2 uker til testgjennomføringen. 2.Pilot I parallell med gjennomføring av akseptansetesten planlegges gjennomføring av pilot, jmf MP3. Det forutsettes at kunden tidlig avklarer aktuelle pilotcase, da det erfaringsvis tar tid. Ihht bilag 5 skal piloteringen gjennomføres i 2-3 utvalgte bydeler/sykehjem. Telenors anbefaling er at det er tilstrekkelig med 1 til 2 tjenestemottakere pr pilot/hovedfunksjon og foreslås gjennomført over 3 uker, med ukentlig statusmøte, hvor siste uke avsettes til oppsummering. Leverandøren etablerer utkast til sjekkliste som ligger til grunn for piloteringen. Sjekklisten påser at pilot dekker nødvendige case for å gi tilstrekkelig erfaring som kan ligge til grunn for godkjenning. Leverandøren tilbyr å gjennomføre jevnlig statusmøter i piloteringsfasen for å svare ut eventuelle spørsmål som måtte dukke opp samt raskt kunne gjøre nødvendige tilpasninger. <u>Forutsetninger for oppstart av pilot:</u> • Akseptansetest er godkjent • Pilotbydel/institusjon/tjenestemottakere er valgt ut • Utstyr er bestilt ○ Vi foreslår at løsning monteres mot slutten av måned 2, så snart resultat fra sikkerhetsgjennomgang og akseptansetest samt avrop fra aktuelle bydeler/sykehjem foreligger. Tidspunkt for montering avtales samtidig som avrop på løsning for øvrig. • Leverandør har gjort nødvendige prekonfigureringer • Løsning er montert • Opplæring er gjennomført • Bør gjennomføres samme uke som pilotoppstart (uke 1, måned 3) • Nettverk tilgjengelig og nettverksporter åpnet • Go-no-go møte er gjennomført <u>Tidsestimater:</u> Oppstart + opplæring uke 1, pilotering uke 2, 3 og 4 samt avslutning og oppsummering i uke 4. Tidsbruk avhenger av antall piloter, tjenestemottakere og tjenesteutøvere som skal involveres. 3.Evaluering og godkjenning	

AS



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI																																																								
Vi anbefaler at det gjennomføres løpende korte evalueringsmøter for å følge opp piloten underveis samt grundig dokumentasjon fortløpende. Etter avsluttet pilot (uke 4, måned 3) gjennomføres et oppsummeringsmøte med fokus på gevinster og forbedringsområder. Evalueringen tar utgangspunkt i både mennesket og organisasjonen.																																																										
9.3 (E3)	Løpende drift: Leverandøren bør ha god leveransekapasitet av tjenesten. Dette innebærer rask og smidig levering etter bestilling fra Kunden, samt gode forutsetninger for skalerbarhet/elastisitet knyttet til leveransebehov. <u>Utformingskrav</u> Leverandøren beskriver sin tilnærming til løpende drift. Beskriv responstid fra bestilling til hovedfunksjonen(e) er tilgjengelig for tjenestemottaker, hvilke aktiviteter som må gjennomføres for at hovedfunksjon skal være tilgjengelig for tjenestemottaker, ansvarsfordeling og tidsestimater, og hva Kunden må legge til rette for/stille med av ressurser for at planen skal kunne gjennomføres (inkl. tidsestimat for Kundens ressursbruk).	JA																																																								
Leverandørens besvarelse: Vi har med utgangspunkt i vår løsning og kundens vedlagte arbeidsprosess utarbeidet et forslag til plan for løpende drift: <table><tr><th>1. Identifisering</th><th>2. Kartlegging</th><th>3. Samtykke</th><th>4. Vedtak</th><th>5. Bestilling</th><th>6a. Montering</th><th>6b. Konfigurerings og tilpasning</th><th>7. Informasjon og opplæring til tjenestemottaker</th><th>8. Demontering og avslutning</th></tr><tr><td colspan="7">A</td><td colspan="2">Opplæring av ansatte</td></tr><tr><td colspan="7">B</td><td colspan="2">Dokumentasjon</td></tr><tr><td colspan="7">C</td><td colspan="2">Kontinuerlig tilpasning etter behov</td></tr><tr><td colspan="4"></td><td colspan="5">D</td><td>Mottak / håndtering av varsler og alarm</td></tr><tr><td colspan="4"></td><td colspan="5">E</td><td>Respons / utrykning</td></tr></table> Figur 1: Arbeidsprosess Før beslutning om oppstart i en ny virksomhet anbefaler vi at det alltid gjennomføres et oppstartsmøte, jmf krav 8.1 og 8.2. Pkt 1 til og med pkt 4, ref listen over, anser vi som en del av kundens interne prosess for å forberede ibruktageelse av velferdsteknologiske løsninger. Telenor ønsker å være en samarbeidspartner på disse områdene og bidrar gjerne med underlagsmaterieell for å sikre et effektivt innføringsløp og best mulig sluttresultat. Ved oppstart på institusjoner og større implementeringer anbefales det å gjennomføre befaring sammen med leverandør i forkant. 5.Bestilling Basert på beslutning om oppstart av Digitalt tilsyn for tjenestemottaker sender kunden en bestilling til leverandør som beskriver hvilken hovedfunksjon det ønskes å gjøre avrop på og ønsket tidspunkt			1. Identifisering	2. Kartlegging	3. Samtykke	4. Vedtak	5. Bestilling	6a. Montering	6b. Konfigurerings og tilpasning	7. Informasjon og opplæring til tjenestemottaker	8. Demontering og avslutning	A							Opplæring av ansatte		B							Dokumentasjon		C							Kontinuerlig tilpasning etter behov						D					Mottak / håndtering av varsler og alarm					E					Respons / utrykning
1. Identifisering	2. Kartlegging	3. Samtykke	4. Vedtak	5. Bestilling	6a. Montering	6b. Konfigurerings og tilpasning	7. Informasjon og opplæring til tjenestemottaker	8. Demontering og avslutning																																																		
A							Opplæring av ansatte																																																			
B							Dokumentasjon																																																			
C							Kontinuerlig tilpasning etter behov																																																			
				D					Mottak / håndtering av varsler og alarm																																																	
				E					Respons / utrykning																																																	

ALS are



Oslo kommune
Helseetaten
Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI
	for montering. 6.Montering, konfigurering og tilpasning Telenor tilbyr montering som en del av vårt tilbud, ved bruk av vår samarbeidspartner som har god kompetanse på dette. Vi forplikter oss til å levere løsningen så raskt som mulig, dog ikke senere enn 3-5 virkedager fra bestilling til løsningen skal være montert og tilgjengelig for kunden. For leveranser som haster vil vi kunne levere neste virkedag. For alle større bestillinger som installasjoner på hele institusjoner krever et grundig forarbeid for vellykket resultat. Her forplikter vi oss til at løsningen skal være montert og tilgjengelig innenfor 12 virkedager. Deretter må kunden selv gjøre nødvendige konfigureringer slik at løsningen er tilpasset den aktuelle tjenestemottaker. Sammen med kamera leveres skilt som monteres for å signalisere at det benyttes kamera for digitalt tilsyn  Smil! Digitalt tilsyn fra Telenor er installert her.  Øvrige forutsetninger: • Opplæring av administratorer/superbrukere (leverandør) • Opplæring av tjenesteutøvere og introduksjon til tjenestemottaker (Kunde) • Konfigurasjon av kundekonto og integrasjon satt opp (leverandør) • Opprettelse av systembrukere (kunde) • Justering av sensorer (kunde) • Utrulling til systembrukere (kunde) • Oppfølgingsmøter (leverandør/kunde) 7.Informasjon og opplæring til tjenestemottaker Leverandøren tilbyr opplæringsmateriell til tjenestemottakere og pårørende som kunden kan distribuere når løsningen tas i bruk. 8.Demontering og avslutning Der tjenestemottaker ikke lenger skal benytte digitalt tilsyn demonterer kunden utstyret og returnerer dette til leverandør, med mindre det er andre tjenestemottakere innenfor samme avrop som skal overta løsningen.	

AS *[signature]*



Oslo kommune
Helseetaten

Seksjon for velferdsteknologi

Krav-nr.	Leverandørens løsningsbeskrivelse – Krav til plan og metode for gjennomføring	JA/NEI

Tabell 9 – Krav til plan og metode for gjennomføring

MS Ake

○

○

AS case

Oslo kommunev/ Helseetaten
Seksjon for velferdsteknologi

Vår dato
18.10.2019

Vår referanse

Deres dato

Deres referanse

Vår saksbehandler
Caroline Cappelen

Revidert tilbud – Leie av teknologi knyttet til digitalt tilsyn

Telenor Norge AS takker for anledningen til å revidere vårt tilbud. Telenor er svært innstilt på vise oss fortjent til å bli leverandør til Oslo kommune. Vi har gjennomgått hele vårt tilbud med tanke på å gi Oslo kommune best mulige forbedringer på viktige områder innen funksjonalitet, brukervennlighet, gjennomføring og pris.

Vedlagt finner dere vårt reviderte tilbud, v3, som i helhet erstatter siste versjon, datert 16.9.2019.

Vi har i dette brevet oppsummert de viktigste forbedringene i vårt reviderte tilbud. I tillegg gir vi en oppdatert informasjon på nylig utvikling om forhold vi mener er relevant for Oslo kommune knyttet til anskaffelsen.

Funksjonalitet

I Delkonkurranse 4 tilbyr vi hendelsesbasert kameratilsyn som en tilleggstjeneste. Dette vil legge til rette for at Oslo kommune kan utnytte fleksibiliteten som ligger i Telenors kamerabaserte tjeneste og dermed sikre best mulig behovsdekning i tjenesten.

Brukervennlighet

Vår beskrivelse av krav omhandlende at systemet bør ha god funksjonalitet knyttet til å holde oversikt over og håndtere varsler, samt se sanntidsstatus på både teknisk status og status relatert til tjenestemottaker, er oppdatert.

Telenors løsning har et alarmmottak hvor alle varsler for tjenestemottakere, både helsevarsler og tekniske varsler, vises i sanntid i samme grensesnitt. Dette sikrer god oversikt for tjenesteyter.

Ved stort volum av varsler er det mulig å sette på filtre i løsningen slik at man bare ser varsler knyttet til en spesifikk tjenestemottaker, eller bare varsler av en spesifikk type, f.eks. kun tekniske varsler.

Denne iboende fleksibiliteten sikrer både god oversikt over de samlede varsler, samt mulighet for å skille teknisk status og status relatert til tjenestemottaker når det er nødvendig.

Gjennomføringsevne

Telenor forstår at forutsigbare leveransetider, samt raske leveranser er viktig for Oslo kommune og ikke minst for mottagerne av tjenestene. Etter dialog med vår leverandør av tjenester knyttet til montering, har vi har oppdatert tilbudet med vesentlig kortere leveransetider.

Vi vil opplyse at vi har svært gode erfaringer med denne leverandør etter samarbeid innen montering, demontering og service av velferdsteknologi i Asker og Bærum for 3000 tjenestemottagere i flere år. Våre erfaringer med leverandøren tilsier at leveransetidene i praksis er godt innunder forpliktende tider og ikke minst at hastebestillinger blir fulgt opp med leveranser samme eller påfølgende dag.

Pris

Vi har gjennomgått strukturen i vårt pristilbud, herunder fordeling av kostnader mellom etablering og løpende drift. Dette har bl.a. medført at vi har kunnet gi en vesentlig forbedret pris i delkonkurranse 4.

Oppdatert informasjon om andre forhold som ansees relevant for anskaffelsen

Velferdsteknologisk knutepunkt (VKP)

Telenor har i tidligere versjon av tilbudet, samt i forhandlingsmøte, påpekt at vi anser at plattformen som tjenesten Telenor Digitalt tilsyn er basert på, Shepherd, har svært gode integrasjonskapabiliteter.

Vi ønsker å oppdatere Oslo kommune med informasjon om at Shepherd-plattformen siden primo september har vært i skarp produksjon for EPJ-integrasjon via VKP med støtte både for Visma Profil og Tieto Gerica journalsystemer. Dagens produksjon gjelder overføring av journalnotater fra helsefaglig responscenter for 3000 tjenestemottagere. Erfaringene så langt er svært gode og flere store kommuner er på vei inn på løsningen. Telenor Digitalt tilsyn vil benytte den samme implementeringen av vår VKP-integrasjon.

Videreutvikling av Neat Novo

Vi har i tidligere informert i styrken og muligheten som ligger i å benytte en felles kommunikasjons-hub på tvers av trygghetsalarm og tilhørende sensorer, digitalt tilsyn og medisinsk avstandsoppfølging. Vårt tilbud inkluderer Neat Novo som kommunikasjons-hub for kameraer og sensorer. Denne inngår i alle delkonkurranser, både til hjemmeboende og på institusjon, med Telenor 4G-kommunikasjon inkludert.

Neat Novo blir løpende testet og sertifisert for medisinske sensorer til bruk innen medisinsk avstandsoppfølging, i tett samarbeid mellom Neat Electronics og Telenor.

Samspill mellom Telenor Digitalt tilsyn og responscenterplattform

Telenor har en tydelig strategi på at alle velferdsteknologi-tjenestene vi tilbyr skal integreres med helsefaglig responscenter.

Vi har denne høsten videreutviklet Digitalt tilsyn slik at løsningen nå er integrert med vår responscenterplattform med oppfølging fra vårt helsefaglige responscenter. Dette er funksjonaliteten som kan overføres til andre responscenterplattformer.

Planlagt kameratilsyn implementeres som kalenderfunksjonalitet i responscenterløsningen hvor operatørene varsles når tilsynet skal gjøres. Sammen med Kristiansand og Grimstad kommune er vi nå i prosess med å teste ut løsningen i skarp drift.

Vi vil også fremheve at vi har kapabilitetene klare til å integrere også hendelsesbasert tilsyn med responscenteret gjennom bruk av SCAIP protokollen. Med dette vil hendelser fra Digitalt tilsyn komme inn på en responscenterplattform, fullintegrert, på samme måte som fra en trykghetsalarm.

Det er også verdt å merke seg at vi er pågående FoU-prosjekt sammen med Bergen kommune, Sintef, TellU og Axis hvor vi tester ut oppfølging av Digitalt tilsyn fra responscenter: <https://www.telenor.no/bedrift/aktuelt/helse/digitalt-tilsyn/> Dette har gitt oss verdifull innsikt i nettopp denne typen integrasjoner.

Prosjektet er en del av det Forskningsråd-støttede prosjektet Smart omsorg, som også Telenor samarbeider med Oslo kommune om, knyttet til Økernhjemmet.

Vi håper at Telenors revidert tilbud er i samsvar med Oslo kommunes forventninger.

Med vennlig hilsen,



Lars Bakken
Leder E-helse, Telenor Norge AS

C

O

the

Approver: Leder Telenor Norge e-helse, Lars Bakken

Sikkerhetshåndbok Telenor Norge e-helse

Versj.nr.	Dato	Utarbeidet/revidert av	Endringsbeskrivelse
1.0	20180701	Amund Lundgaard	Ny sikkerhetshåndbok for Telenor Norge e-helse påbegynt etter mal basert på Sikkerhetshåndbok for Telenor Norge
1.1	20180816	Amund Lundgaard	Komplettert kapittel 2-8.
1.2	20190520	Amund Lundgaard	Oppdatert kap 3 iht ny organisering Telenor Norge e-helse, revidert sikkerhetsstrategi.

MS ACE

Innhold

1	INNLEDNING OG OMFANG.....	3
1.1	Distribusjon	4
1.2	Referanser	4
2	SIKKERHETSMÅL OG STRATEGI.....	4
2.1	Mål for sikkerhetsarbeidet	4
2.2	Sikkerhetsstrategi	5
2.3	Kvartalsvise målsetninger.....	6
2.4	Nivå for akseptabel risiko	6
3	ORGANISERING AV SIKKERHETSARBEIDET.....	10
3.1	Telenor Norge sikkerhetsorganisasjon	11
3.2	Telenor Norge e-helse sikkerhetsorganisasjon	12

AS me

1 Innledning og omfang

Dette dokument utgjør lokal sikkerhetshåndbok for *Telenor Norges e-helse*, organisert under Telenor Norge, divisjon Bedrift, avdeling Smart Digital, enhet for e-helse. Tjenestene utgjør både tjenester rettet mot kommune, sykehus og øvrige offentlige og private helseaktører. Telenors ordinære telekommunikasjonstjenester for fast og mobil kommunikasjon regnes i denne sammenheng ikke som e-helsetjenester selv om de skulle ytes til en helsevirksomhet.

Telenor Norges sikkerhetskrav, målsetninger, overordnet organisering, prosedyrer, maler og retningslinjer er gjeldende, med mindre annet er angitt i dette dokumentet.

Dokumentet er etablert for å sikre lokal innføring av overordnede sikkerhetskrav i Telenor Norge, angitt i *Sikkerhetshåndbok for Telenor Norge* («Sikkerhetshåndboken»), samt ivaretagelse av spesifikke krav for e-helsetjenestene, og er styringsdokumentet for hvordan Telenor Norge e-helse skal utøve vårt sikkerhetsarbeid, og angir sikkerhetskrav for aktiviteter som er av sikkerhetsmessig betydning.

Målgruppe er alle ansatte i Telenor Norge e-helse, andre ansatte i Telenor Norge som utfører oppgaver på vegne av Telenor Norge e-helse, samt innleide som i tidsbegrenset periode utfører oppgaver på vegne av Telenor Norge e-helse.

Dokumentet beskriver **hva** kravene er og hvem som har **ansvar** for ivaretagelse. Dokumentet henviser til en rekke prosedyrer som detaljerer kravene til sikkerhet innen spesifikke områder. Prosedyrene beskriver **hvordan** kravene skal ivaretas.

Dokumentet og underliggende dokumentasjon og prosedyrer utgjør Telenor Norge e-helses dokumentasjon på *tilfredsstillende informasjonssikkerhet* iht Personopplysningsloven, samt dokumentasjon på at nødvendige tekniske og organisatoriske tiltak er iverksatt for å understøtte at Telenor Norge e-helse yter forsvarlig helsehjelp i våre bemanningsbaserte tjenester.

Viktigste overordnede forskjeller i rammer for *Sikkerhetshåndboken* og dette dokument er at Telenor Norge e-helse ikke produserer egne tjenester undergitt *Ekomloven* og *Sikkerhetsloven*. Tjenestene som produseres er enten

- helsetjenester som inngår i kundenes helse- og omsorgstjenester iht. *Lov om kommunale helse- og omsorgstjenester (Helse og omsorgstjenesteloven)*, *Lov om helsepersonell m.v. (helsepersonelloven)* og *Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)*, eller
- teknologitjenester som behandler personopplysninger iht *Lov om behandling av personopplysninger (Personopplysningsloven)* og iht *Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)* mv.

Særegent for Telenor Norge e-helse er at Telenor Norge utelukkende er Databehandler på vegne av Dataansvarlig, Telenor Norge har ikke eget Behandlingsansvar for person- eller helseopplysninger. Telenor Norges forpliktelser som Databehandler er dokumentert i inngåtte Databehandleravtaler.

Handwritten signature and initials.

Spesifikke funksjonelle og tekniske krav til teknologitjenestene er samlet angitt i *Norm for informasjonssikkerhet i helse- og omsorgssektoren* («Normen»), på bakgrunn av underliggende lovgivning i Personopplysningsloven, relevant helselovgivning mv. og blir ikke gjengitt i dette dokument.

1.1 Distribusjon

Dokumentet i sin helhet er klassifisert som INTERNAL / INTERN iht. Telenor Norges retningslinjer for gradering av informasjon.

Dokumentet i sin helhet kan presenteres for Dataansvarlige eller andre med legitim interesse, men ikke distribueres.

Samlet innholdsfortegnelse, samt kapittel 1, 2 og 3 kan distribueres til Dataansvarlige eller andre med legitim interesse.

1.2 Referanser

- Telenor Norge sikkerhetshåndbok
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)
- Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven)
- Lov om helsepersonell m.v. (helsepersonelloven)
- Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)
- Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)
- Norm for informasjonssikkerhet i helse- og omsorgssektoren
- Telenor Norge e-helse signerte databehandleravtaler

2 Sikkerhetsmål og strategi

2.1 Mål for sikkerhetsarbeidet

Telenor Norge E-helse er en totalleverandør av velferdsteknologi og –tjenester, samt en rekke øvrige e-helsetjenester til norske helsevirksomheter. Våre overordnede sikkerhetsmål omfatter alle aspekter av tjenesten, inkludert helsefaglige og andre bemanningsbaserte tjenester i vår portefølje, mens sikkerhetsmål om forsvarlig IKT er mer spesifikke for den delen av tjenesteporteføljen som er basert på utstyr og programvare.

2.1.1 Overordnede sikkerhetsmål

Telenor Norge e-helse har pasientsikkerhet og IKT-sikkerhet som vår høyeste prioritet og vårt sikkerhetsarbeid skal sikre at

- kundenes pasienter og tjenestemottakere mottar forsvarlig helsehjelp, og ikke opplever at Telenors tjenester forringer deres frihet, trygghet eller verdighet i hverdagen.

MS

- kundenes plikter som dataansvarlige og Telenors plikter som databehandler, er ivaretatt på beste måte.
- Telenors lovnader om å opptre som ansvarlig samfunnsaktør igjennom å maksimere telekommunikasjonens samfunnsnytte, skape verdier for hele samfunnet og bidra til en bærekraftig fremtid, er ivaretatt.

2.1.2 Sikkerhetsmål om forsvarlige helsehjelp

Telenor Norge e-helse skal igjennom systematisk forebyggende sikkerhetsarbeid, velorganisert drift, samt læring og forbedring etter uønskede hendelser sikre at

- våre tjenester oppfyller relevante lovkrav, samt anerkjente faglige anbefalinger fra offentlige myndigheter eller andre autoriteter.
- vi besitter tilstrekkelig bemanning med riktig tverrfaglig sammensatt kompetanse og riktig opplæring til å yte forsvarlig helsehjelp og til å utvikle, drifte og levere e-helseløsninger, støtteverktøy, installasjonstjenester og helsefaglige tjenester som understøtter kundens forutsetninger for å gi forsvarlig helsehjelp.
- vi holder en høy etisk standard og yter tjenester med konsekvent kvalitet - behandle hver episode individuelt og uhildet av og levere samme kvalitet på samme tjeneste, uavhengig av kunde.

2.1.3 Sikkerhetsmål om forsvarlig IKT

Telenor Norge e-helse skal igjennom systematisk forebyggende sikkerhetsarbeid, velorganisert drift, samt læring og forbedring etter uønskede hendelser, sikre tilstrekkelig

- konfidensialitet og integritet om person-, tjeneste- og kundeopplysninger.
- integritet på person-, tjeneste- og kundeopplysninger, herunder alle konfigurasjoner og variasjoner i tjenesteoppsettet kunde for kunde.
- tilgjengelighet på opplysninger og tjenester, nødvendig for å yte forsvarlig helsehjelp og møte inngåtte kundeforpliktelser.

2.2 Sikkerhetsstrategi

Telenor Norge e-helse sikkerhetsstrategi beskriver hvordan overordnede og spesifikke sikkerhetsmål skal nås. Sikkerhetsstrategien gjelder for alle tjenester som leveres av Telenor Norge e-helse, og omfatter både den organisatoriske enheten «e-helse», forholdet til omkringliggende funksjoner og tjenester i og fra Telenor Norge, og underleverandører og partnere.

1. Telenor Norge e-helse skal forvalte et områdespesifikt praktisk orientert styringssystem i form av en sikkerhetshåndbok med tilhørende støttedokumentasjon inn under rammene gitt av Telenor Norges overordnende styringssystem for informasjonssikkerhet og generelle sikkerhetshåndbok med tilhørende rutiner, prosedyrer og støtteverktøy.

HS *AKC*

2. Telenor Norge e-helse skal drive risikodrevet forbedring. En oppdatert risikovurdering per tjeneste skal være driver for både kontinuerlig forbedring og prioritering av større tiltak i form av prosjekter.
3. Telenor Norge e-helse skal ha en tydelig organisering med godt definerte roller og tilhørende ansvar, og tilstrekkelig bemanning og kompetanse til å fylle alle roller i organisasjonen. Den enkelte skal utøve sin rolle iht. til gjeldende sikkerhetskrav og den enkeltes kompetanse skal holdes jevnlig oppdatert.
4. Telenor Norge e-helse holder sikkerhet som et kollektivt ansvar. Enhver ansatt er ansvarlig for nye identifiserte trusler eller sårbarheter en blir kjent med, inntil ansvaret er overlevert annen ansvarlig.
5. Telenor Norge e-helse erkjenner at uønskede hendelser vil kunne inntreffe, men skal benytte alle uønskede hendelser som kilde for ny læring og forbedring. Øvelser på håndtering av uønskede hendelser skal avholdes jevnlig.
6. Telenor Norge e-helse er en del av Telenor Norge som besitter det sterkeste kompetansemiljøet på IKT-sikkerhet i landet, og har markedsledende standardiserte sikkerhetsprodukter og tjenester. Vi skal benytte Telenor Norges kompetanse og standardprodukter og -tjenester der dette er hensiktsmessig.
7. Telenor Norge e-helse skal velge underleverandører og partnere med overbevisende, veldokumentert sikkerhetspraksis og dokumentert sterk historikk, både innen forebyggende sikkerhetsarbeid og evne til å respondere på og forbedre seg basert på læring etter uønskede hendelser. Virksomheter med styringssystem for informasjonssikkerhet sertifisert iht ISO 27001 av anerkjent sertifiseringsinstans foretrekkes.

2.3 Kvartalsvise målsetninger

Telenor Norge e-helse fastsetter kvartalsvise prioriteringer og målsetninger for all planlagt aktivitet nærmeste kvartal, dette inkluderer også sikkerhetsmessige målsetninger og forbedringstiltak.

Innspill til prioriteringer, målsetninger og forbedringstiltak meldes fra den enkelte ansvarlige i rolle iht. kapittel 3. *Organisering av sikkerhetsarbeidet*, til leder e-helse iht. plan og milepæler for kvartalsplanlegging. Innspill skal være begrunnet i oppdatert dokumentert risikoanalyse for aktuell tjeneste.

2.4 Nivå for akseptabel risiko

Nivå for akseptabel risiko er fastsatt for kategoriene Personopplysningssikkerhet,

AS vane

Pasientsikkerhet. Risiko skal vurderes og klassifiseres iht Telenor Norge e-helse malverk for risikoanalyse. Malverket er basert på Telenor Norges malverk, justert for anbefalinger i Normen, Faktaark nr 5. Fastsette nivå for akseptabel risiko.

Sannsynlighet og Konsekvens skal vurderes basert på eksisterende teknologi, rutiner kontrolltiltak og ikke forutsette at ytterligere tiltak er iverksatt.

Skala for vurdering av kritikalitet er:

Rød sone – Pri 1: Overskrider risikotoleranse. Tiltak skal identifiseres, dokumenteres og iverksettes umiddelbart.

Gul sone – Pri 2: Overskrider ikke risikotoleranse. Tiltak skal være identifisert og dokumentert og inngå i kvartalsvis prioritering og planlegging iht. kap. 2.3.

Grønn sone – Pri 3: Overskrider ikke risikotoleranse. Tiltak kan være identifisert, dokumentert og inngå i kvartalsvis prioritering og planlegging iht. kap. 2.3.

Uavhengig av prioritet bør det alltid være risikoreduserende tiltak identifisert og iverksatt for å sikre at samlet risiko for Telenor Norge e-helse er redusert til laveste mulige nivå.

		Sannsynlighet			
		Usannsynlig (1)	Mindre sannsynlig (2)	Mulig (3)	Sannsynlig (4)
Konsekvens	Kritisk (4)				
	Alvorlig (3)				
	Moderat (2)				
	Ubetydelig/ingen (1)				
(årlig)		< 15%	15-50%	50-85%	> 85%

Figur 1 Nivå for akseptabel risiko

2.4.1 Klassifikasjon Konsekvens – Personopplysnings- og pasientsikkerhet

Følgende klassifikasjon av konsekvens skal benyttes ved risikovurderinger

Kritisk (4)	Tap av liv ELLER
	Irreversibel alvorlig forverring av pasienters helse ELLER
	Irreversibel alvorlig negativ påvirkning på den enkeltes livskvalitet ELLER

KU Ake

	Fullt uautorisert innsyn eller mulighet for endring av alle helse- og personopplysninger ELLER Uopprettelig økonomiske tap for den enkelte ELLER Kritisk informasjon mangler i nødvendige person-/helseopplysninger for tjenesten ELLER Reduksjon/bortfall av kritisk system og/eller kritisk funksjonalitet i system forekommer i mer enn 2 timer ELLER Reduksjon/bortfall av administrativt system og/eller administrativ funksjonalitet i kritisk system forekommer i mer enn 24 timer
Alvorlig (3)	Kortvarig moderat eller irreversibel mindre forverring av pasienters helse ELLER Kortvarig moderat eller irreversibel mindre negativ påvirkning på den enkeltes livskvalitet ELLER Alvorlig negativ påvirkning og krenking av personlige integritet, renommé eller rykte ELLER Uautorisert innsyn i enkelte i helse- og personopplysninger, med mulighet for endring ELLER Uautorisert innsyn i enkelte i helse- og personopplysninger for et stort antall registrerte ELLER Viktig informasjon mangler i nødvendige person-/helseopplysninger for tjenesten ELLER Brukertilganger tildeles person uten tjenstlig behov (uavhengig av om den blir benyttet eller ikke) ELLER Reduksjon/bortfall av kritisk system og/eller kritisk funksjonalitet i system forekommer i inntil 2 timer ELLER Reduksjon/bortfall av administrativt system og/eller administrativ funksjonalitet i kritisk system forekommer i mer enn 12 timer
Moderat (2)	Mindre og kortvarig, men reversibel, forverring av pasienters helse ELLER Mindre og kortvarig, men reversibel, negativ påvirkning på den enkeltes livskvalitet Mindre negativ påvirkning og krenking av personlige integritet, renommé eller rykte ELLER Mindre og midlertidig, men opprettelig, økonomiske tap for den enkelte ELLER Uautorisert innsyn kun i enkelte i helse- og personopplysninger ELLER Noe informasjon mangler i nødvendige person-/helseopplysninger for tjenesten

Handwritten signature/initials

	ELLER Reduksjon/bortfall av kritisk system og/eller kritisk funksjonalitet i system forekommer i inntil 30 minutter ELLER Reduksjon/bortfall av administrativt system og/eller administrativ funksjonalitet i kritisk system forekommer i mer enn 12 timer
Ubetydelig/Ingen (1)	Ingen fare for forverring av pasienters helse OG Ingen negativ påvirkning på den enkeltes livskvalitet OG Ingen negativ påvirkning og krenking av personlige integritet, renommé eller rykte OG Ingen økonomiske tap for den enkelte OG Intet uautorisert innsyn i helse- og personopplysninger OG Nødvendige helseopplysninger for tjenesten er komplett OG Reduksjon/bortfall av system og/eller viktig funksjonalitet i system forekommer ikke

2.4.2 Klassifikasjon Sannsynlighet

Følgende klassifikasjon av sannsynlighet skal benyttes ved risikovurderinger

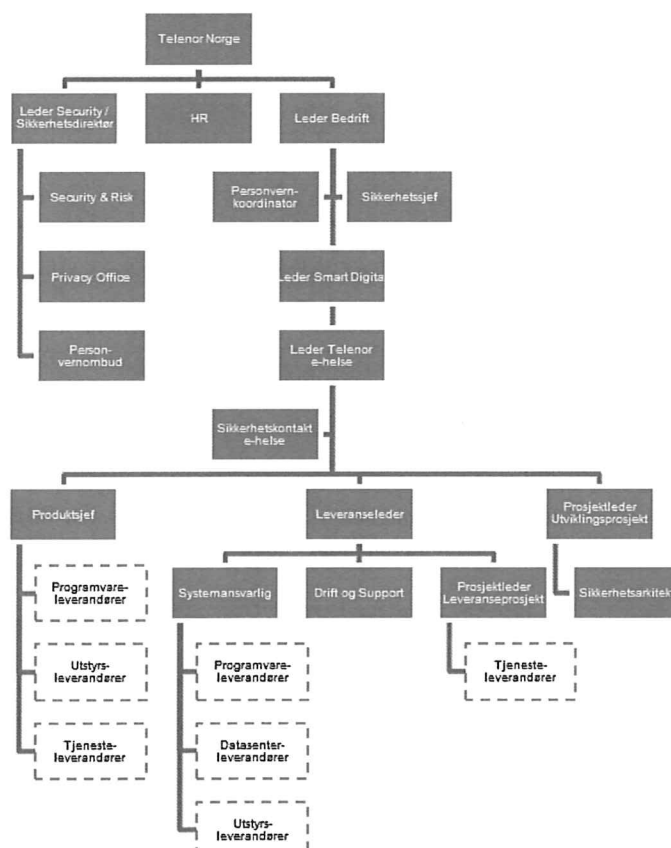
Sannsynlig (4)	Autoriserte brukere kan utløse scenariet ved et uhell. Uautoriserte brukere trenger ikke spesiell kompetanse, utstyr eller hjelp fra en ansatt for at scenariet skal inntreffe. Mer enn 85% sannsynlighet for at scenariet vil inntreffe ila ett år.
Mulig (3)	Autoriserte brukere må handle uaktsomt for at risikoscenariet skal inntreffe. Uautoriserte brukere trenger ikke spesiell kompetanse eller hjelp fra en ansatt for å utløse risikoscenariet, men det vil kreve vesentlig tidsbruk eller utstyr. Mer enn 50%, men mindre enn 85% sannsynlighet for at scenariet vil inntreffe ila ett år.
Mindre sannsynlig (2)	Autoriserte brukere må handle med forsett for at scenariet skal inntreffe.

HS are

	Uautoriserte brukere trenger spesiell kompetanse og spesielt utstyr, men trenger ikke hjelp fra en ansatt for at scenariet skal inntreffe. Mer enn 15%, men mindre enn 50% sannsynlighet for at scenariet vil inntreffe ilt ett år.
Usannsynlig (1)	Autoriserte brukere må handle med forsett og få hjelp fra annen autorisert bruker for at scenariet skal inntreffe. Uautoriserte brukere trenger spesiell kompetanse, spesielt utstyr og få hjelp fra en ansatt for at scenariet skal inntreffe. Mindre enn 15% sannsynlighet for at scenariet vil inntreffe ilt ett år

3 Organisering av sikkerhetsarbeidet

Kapitlet beskriver Telenor Norge e-helse sikkerhetsorganisasjon og ansvar. Overordnet organisering er illustrert i figuren under. Underleverandører og partnere er illustrert inn med stiplede linjer.



Figur 2 Telenor Norge e-helse sikkerhetsorganisasjon

AS are

3.1 Telenor Norge sikkerhetsorganisasjon

Sikkerhetsdirektør - Telenor Norges Sikkerhetsdirektør er prosesseier for støtteprosess sikkerhet. Dette innebærer et overordnet ansvar for å stille krav, bistå og følge opp implementering av nødvendig sikkerhet i forretningsprosessene, samt å rapportere på sikkerhetsstatus til ledelsen i Telenor Norge. Sikkerhetsdirektøren har en premissgivende, rådgivende og kontrollerende rolle.

Sikkerhetssjef i Telenor - Norge Business - Sikkerhetssjef har en premissgivende, rådgivende og kontrollerende rolle og skal følge opp implementering av sikkerhetskravene i divisjonene.

Prosesseier HR - har et overordnet ansvar for å sørge for at krav til personellsikkerhet og bevisstgjørende- og holdningsskapende sikkerhetsopplæring av alle ansatte, blir ivaretatt i støtteprosess HR (ref. Sikkerhetshåndboken kap. 2.3).

Personvernombud – Personvernombudet er felles med øvrige tjenester i Telenor Norge. Personvernombudene har en rådgivende og kontrollerende rolle. Ombudenes oppgave er å sikre at Telenor følger personopplysningsloven med forskrift. Personvernombudet skal være en ressursperson både for virksomheten og de registrerte i spørsmål vedrørende personvern i Telenor. Personvernombudet skal bl.a.:

- Være kontaktpunkt mellom Telenor i Norge og Datatilsynet
- Bistå registrerte

Lokal personvernkontakt (Local Privacy Officer) – Telenor Norge, divisjon Bedrift, har en egen personvernkontakt. Lokal personvernkontakt er divisjonens kontakt inn mot Privacy office Telenor Norge og skal bl.a.:

- Være rådgivende instans i forbindelse med prosesser som omhandler behandling av personopplysninger
- Bidra til at det gjennomføres en årlig internkontroll av selskapets behandling av person-opplysninger
- Overvåke samsvar med gjeldende regelverk
- Melde vesentlige avvik til ledelse, Personvernombudet og Group Privacy Officer og følge opp at eventuelle avvik blir lukket.

Linjeleder - Linjeleder skal påse at sikkerhetskrav er implementert og etterleves i egen linjeenhet. Dette omfatter å:

- Ha oversikt over hvilke verdier (assets) han/hun er satt til å forvalte og hva det betyr i forhold til mandat og ansvarsområde
- Ha oversikt over sårbarheter som er knyttet til verdiene, hvilke trusler som kan påvirke negativt, og derav kunne belyse viktige risikoforhold

Handwritten initials and signature in the bottom right corner.

- Gi tilstrekkelig sikkerhetsopplæring til medarbeidere
- Etablere nødvendige sikkerhetsrutiner i prosessene
- Ha nødvendig kontroll med etterlevelse av sikkerhetskrav

Linjeledelse utøves av leder for Divisjon Bedrift, med delegert ansvar til avdelingsdirektør for avdeling Smart Digital.

3.2 Telenor Norge e-helse sikkerhetsorganisasjon

3.2.1 Premissgivende roller

Premissgivende; bestemmer krav til nødvendig beskyttelse av verdiene;

Leder e-helse – utøver rollen som **Prosesseier** og har både en premissgivende og kontrollerende rolle. Bestemmer krav til nødvendig beskyttelse av verdiene, Telenors nivå av akseptabel risiko, godkjenner lokalt styringssystem og internkontroller.

3.2.2 Utøvende roller

Utvøvende; er ansvarlig for praktisk gjennomføring av informasjonssikkerhetsarbeidet, inkludert valg av konkrete sikkerhetstiltak;

Leveranseleder – overordnet ansvar for gjennomføring av alle konkrete tiltak, både preventive, reaktive og kontrollerende, for alle produkter og tjenester under ordinær kontrakt med kunde – ikke innovasjonsprosjekter. Beslutter administratorrettigheter til alle produksjonssystemer.

Systemansvarlig – spesifikt ansvar for ivaretagelse av sikkerhetskrav for IKT-systemer i sin portefølje, inkludert gjennomføring av alle konkrete tiltak, både preventive, reaktive og kontrollerende, for IKT-systemer i sin portefølje, inkludert tilhørende produkter og tjenester fra underleverandører. Forvalter administratorrettigheter til alle produksjonssystemer. Ansvar for

Produktsjef - spesifikt ansvar for ivaretagelse av sikkerhetskrav for sine produkter inkludert gjennomføring av alle konkrete tiltak, både preventive, reaktive og kontrollerende, for produkter og tjenester i sin portefølje, inkludert tilhørende produkter og tjenester fra underleverandører. Skal normalt ha administratortilgang til produksjonssystemer for sine produkter.

Prosjektleder Utviklingsprosjekter – ansvarlig for at det er etablert sikkerhets- og personvernkrav til tjenesten, gjennomføre vurdering av personvernkonsekvenser, sikre sikkerhetsmekanismer og personvern i design, sikre tilstrekkelig testing og riktige testdata, etablere dokumentasjon, og gjennomføre forsvarlig utprøving.

Sikkerhetsarkitekt Utviklingsprosjekter – kan ha delegert ansvar fra prosjektleder utviklingsprosjekter dersom rollen er etablert innenfor prosjektet og bemannet med tilstrekkelig kapasitet med riktig kompetanse.

AS Ace

Prosjektleder Leveranseprosjekter – ansvarlig for at det er gjennomført kundespesifikk vurdering av innføringsrisiko og personvernkonsekvenser, at det etableres kundespesifikk dokumentasjon, opplæring og rutiner.

Drift og support – Den enkelte ansatt, inkludert innleide/konsulenter, har ansvar for å gjøre seg kjent med sikkerhetskrav og følge disse i utøvelsen av sitt arbeid.

Lokal Sikkerhetskontakt e-helse – ansvarlig for forvaltning av sikkerhetshåndbok i tråd med retningslinjer fra Telenor Norge, regulatoriske krav og inngåtte kundeforpliktelser. Metode- og verktøyansvar for risikovurderinger, internkontroll, interne sikkerhetsrevisjoner mv.

3.2.3 Utøvende roller fra Telenor Norge

Tjenester hvor Telenor Norge e-helse forholder seg til Telenor Norge som leverandør og ikke som del av sikkerhetsorganisasjonen. Representert i organisasjonskart som stiplede bokser.

Telenor Bedrift Storkunde Feilmottak overvåkning applikasjoner – Overvåkning av applikasjoner og kommunikasjonstjenester i sin portefølje iht tjenesteavtale. Respondere på hendelser iht plan med hovedoppgave å opprettholde eller gjenopprette ordinære drift.

Telenor Bedrift M2M Mobilkommunikasjon tale/data – Overvåkning av mobilabonnement og databruk mtp. risiko for misbruk/svindel, struping som følge av overforbruk mv.

Telenor IPT telefoni – Oppfølging av tjenestekvalitet, analyse og tiltak ifbm uønskede hendelser på IPT-telefonitjenester for responsplattform.

Telenor Internett / Nordic Connect datakommunikasjon - Oppfølging av tjenestekvalitet, analyse og tiltak ifbm uønskede hendelser på IPT-telefonitjenester for responsplattform.

Telenor Security Operations Center - overvåkning av Telenors nett og infrastruktur

3.2.4 Øvrige utøvende funksjoner

Sikkerhetsfunksjoner som utøves av underleverandører og partnere iht. tjenesteavtaler eller Databehandleravtaler regnes ikke som del av Telenor Norge e-helse sikkerhetsorganisasjon, men følges opp igjennom kontrolltiltak iht. ansvar beskrevet under avsnitt om kontrollerende roller. Representert i organisasjonskart som stiplede bokser.

3.2.5 Kontrollerende roller

Leder e-helse – utøver rollen som **Prosesseier** og har både en premissgivende og kontrollerende rolle. Ansvarlig for gjennomføring av sikkerhetsgjennomganger og vurdering av overholdelse av sikkerhetshåndbok og underliggende retningslinjer og prosedyrer.

Produktsjef – har verdikjedeansvar for produkter i sin portefølje. Ansvarlig for oppfølging av underleverandører og deres sikkerhetspraksis og tiltak iht tjenesteavtaler og Databehandleravtaler.

AS Mre

3.2.6 Rådgivende roller

Lokal Sikkerhetskontakt e-helse – har skal sikre at Telenor Norge e-helse har tilstrekkelig kompetanse om sektorspesifikke regulatoriske krav, kjennskap til generelt trusselbilde, anbefalt sikkerhetspraksis mv. og være rådgiver for alle utøvende roller.

Produktsjefer og/eller rådgivere Telenor basisprodukter: M2M mobilkommunikasjon, IPT telefoni, Internt / Nordic Connect datakommunikasjon mv – rådgivning om egenskaper og begrensninger ved aktuelle produkter, produktveikart, risikovurderinger mv.

Produktsjefer og/eller rådgivere hos programvare-, utstyrs-, eller datasenterleverandører: rådgivning om egenskaper og begrensninger ved aktuelle produkter, produktveikart, risikovurderinger mv.

KS MCE