Pasientvarsling med tilhørende tjenester Trondheim kommune

2020 PAVA SSA-V Bilag 1 Leverandørens løsningsspesifikasjon Krav ved ekstern drift

Innhold

1 Generelt

Dette bilaget og svardelen Bilag 2 Krav ved ekstern drift gjelder løsninger der drift / applikasjonsdrift / vedlikehold foregår fra leverandørens servere / sky. Kravene i Bilag 2 Krav ved ekstern drift gjelder i tillegg til krav i Bilag 6 Administrative bestemmelser.

Kravene omfatter egenskaper og kvaliteter ved hvordan løsningen leveres. Kravene omhandler løsningens sikkerhet, robusthet og tilgjengelighet. I tillegg til den tekniske plattformen, omhandler dette også organisering og kvalitet på løpende drift og vedlikehold fra Leverandøren.

1.1 Prinsipper og føringer

Sikkerhetsprinsipper og -krav for IKT-infrastruktur er en sammenstilling av nødvendige prinsipper og krav for å oppnå tilfredsstillende informasjonssikkerhet. Prinsippene er bygget over tid og har tett tilknytning til Oppdragsgivers arkitekturprinsipper og løsningsdesign https://sites.google.com/trondheim.kommune.no/arkitektur/prinsipper.

1.2 Norm for informasjonssikkerhet i Helse- og omsorgstjenesten

Oppdragsgiver har forpliktet seg til å følge den til enhver tid gjeldende versjonen av Normen.

Løsningen og Leverandør av løsningen, skal i utvikling, videreutvikling og drift / vedlikehold, ivareta krav og føringer gitt i gjeldende Norm for informasjonssikkerhet i helsesektoren (Normen).

Normens faktaark beskriver hvordan Leverandøren kan oppfylle sentrale krav i Normen og gi praktisk veiledning. Det forutsettes at Leverandøren aktivt forholder seg til Normens faktaark.

2 Krav til drift og sikkerhet - driftstjenester

2.1 Overordnede krav

Krav nr.	Kravbeskrivelse	Krav-kode M, B	Svar-kode J/N/T	Leverandøren svarer i
1	**Robust og skalerbar driftsplattform** Leverandøren bes beskrive IT-driften av løsningen i henhold til følgende: ● I hvilken grad driftsplattformen følger relevante bransjestandarder. ● I hvilken grad driftsplattformen er velprøvd med kommersiell utbredelse, og i hvilken grad den er geografisk redundant ● I hvilken grad driftsplattformen leverer skalerbarhet, tilgjengelighet og kontinuerlig drift ● I hvor stor grad plattformen har mekanismer og prosesser for monitorering av ytelse, feil og brukeropplevd responstid	B		Bilag 2

	● I hvilken grad driftsplattformen har mekanismer for å detektere sikkerhetshendelser (IDS/IPS, bli utsatt for ondsinnet kode, applikasjonsbrannmurer, DDoS-beskyttelse, tiltak som forhindrer eller sikrer at man oppdager uautoriserte eller ikke-planlagte endringer). ● I hvilken grad driftsplattformen har mekanismer for å håndtere privilegert tilgang til driftsmiljø, overvåkning, sporbarhet og kontroll med egne driftsressurser og tredjeparter.			
2	**Rutiner for sikker og robust IT-drift** Leverandøren bes beskrive IT-driften av løsningen i henhold til følgende: • I hvilken grad driftsorganisasjonen følger bransjestandarder for organisering og drift av løsningen (for eksempel ITIL, KCS, HDI, DevOps eller tilsvarende) • I hvilken grad driftsorganisasjonen har gode og dokumenterte rutiner for styring og kvalitetssikring av driften av løsningen, herunder ressurs- og ansvarsfordeling og rutiner ved uforutsette hendelser – gjerne basert på etablerte standarder • I hvilken grad driftsorganisasjonen har organisering og prosesser som sikrer løsningen og driftsplattformen mot sikkerhetshendelser, inkludert loggovervåkning, loggsammenstilling, evt. sikkerhetsanalytikere sin deltakelse og arbeid med løsningen, planverk for respons og håndtering av sikkerhetshendelser • I hvilken grad Leverandøren har rutiner og prosesser for å håndtere privilegert tilgang til driftsmiljø, herunder lokaler, overvåkning, sporbarhet og kontroll med egne driftsressurser og tredjeparter. Beskrivelsen bør også dekke sikring mot villede handlinger (innbrudd, sabotasje) • I hvilken grad Leverandøren har effektive prosesser for å gjennomføre sårbarhetsanalyser, og prioritering og utrulling av sikkerhetspatcher • I hvilken grad Leverandøren har gode rutiner for håndtering av driftsavbrudd for integrasjoner for	B		Bilag 2

	løsningen, som synliggjør at Leverandøren bidrar til å identifisere hvor feilen ligger i løsningen (og eventuelt mot tredjeparter), samt varsling av Kunden om dette • I hvilken grad Leverandøren etablerer og vedlikeholder en dokumentert kontinuitets- og beredskapsplan som dekker krisesituasjoner, håndtering av sikkerhetsbrudd, sikkerhetskopi- og reservedriftsløsninger for løsningen. Det inkluderer i hvilken grad planene holdes oppdatert gjennom endringer og regelmessig test og øvelse • I hvilken grad Leverandøren dokumenterer og vedlikeholder en backup-policy og rutiner for backup for all informasjon i driftsløsningen, som skal ivareta at det ikke aksepteres tap av data. ● I hvilken grad Leverandøren dokumenterer og overvåker kapasitet, automatiske målinger og driftsstabilitet på IKT-tjenester og infrastruktur i driftsløsningen Kunden ønsker korte og konsise svar. Beskrivelsen av kravet bør ikke overstige 4 sider. Innhold/omfang av eventuelle andre standarder eller sertifiseringer enn de som er nevnt i kravet, bør gjøres tilgjengelig for Kunden på forespørsel.			
3	**Penetrasjonstester** Leverandøren beskriver sitt regime for å gjennomføre penetrasjonstester på løsningen (i egenregi eller av underleverandør). Kunden foretrekker at penetrasjonstester gjennomføres iht. anerkjent metodikk for penetrasjonstesting, eksempelvis NIST SP800-115, og dekke kritiske komponenter i løsningen. Testene bør dekke både interne og eksterne angrepsvektorer, infrastruktur og applikasjoner, og gjennomføres av kvalifisert personell	B		Bilag 2
4	**Kundens sikkerhetstesting** Kunden, eller tredjepart utpekt av Kunden, skal ha rett til å gjennomføre sikkerhetstester av løsningen så lenge dette	M		

	ikke innebærer unødig risiko eller uforholdsmessig påvirker løsningens kapasitet			
5	**Kundesegmentering** Leverandøren skal sikre at det er full separasjon mellom informasjon fra ulike Kunder. Data fra ulike kunder/behandlingsansvarlige skal være skilt fra hverandre på en sikker måte. Leverandøren skal beskytte mot at feil i konfigurasjon, feil i administrasjonsgrensesnittet, menneskelige feil eller ondsinnede handlinger og angrep fører til at det oppstår datalekkasje mellom ulike kunder eller mellom produksjons- og testmiljøer. Leverandøren bes beskrive hvordan dette håndteres	M (beskrives)		Bilag 2

2.2 Informasjon om nedetid

Krav nr.	Kravbeskrivelse	Krav-kode M, B	Svar-kode J/N/T	Leverandøren svarer i
1	**Informasjon om nedetid** Det er ønskelig med løpende informasjon til Kunden og Kundens brukere ved uforutsette driftsforstyrrelser, inkludert når det forventes at tjenesten igjen er fullt operativ. Leverandøren beskriver informasjonsrutiner mot Kunden og Kundens IT Brukerhjelp	B		Bilag 2

2.3 Miljømessig sikkerhet

Krav nr.	Kravbeskrivelse	Krav-kode M, B	Svar-kode J/N/T	Levre andøren svarer i
1	**Sikkerhet drift av løsningen** Leverandøren beskriver hvordan drift av løsningen er sikret med tanke på miljømessige trusler og avvik, herunder: ● Miljømessige hendelser (brann, vanninntrengning, jordskjelv, strømbrudd, eksplosjoner m.v.) Besvarelsen begrenses til 1/2 sider.	M (beskrives)		Bilag 2