Videreutvikling av Aktør- Booking- og Tilskuddsbasen

SSA-O Bilag 1 - Vedlegg B Kravtabell Felles krav til produkt funksjonalitet, produktkvalitet og prosesskrav

Felles krav til produktfunksjonalitet, produktkvalitet og prosess		
KravNr.	**Kravområde**	**Krav til løsning**
Felles produktfunksjonalitet		
FK-4.1.1	ID-porten	Ved integrasjon mot ID-porten skal ID-portens retningslinjer for utforming benyttes, ref. [https://www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/id-porten]
FK-4.1.2	ID-porten	Ved integrasjon mot ID-porten skal integrasjonen valideres iht. ID-portens krav til verifikasjon av integrasjoner, ref. [https://www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/id-porten]
FK-4.1.3	Opplæring	Leverandøren skal kunne gi kundens nøkkelpersoner opplæring i bruk av løsningen etter nærmere avtale
FK-4.1.4	Personvern	Personopplysninger må håndteres i tråd med EU-s nye personvernforordning (GDPR)
FK-6.1.1	Offentlig kartgrunnlag	Ved bruk av kartdata skal det offentlige kartgrunnlaget brukes. Se https://dok.geonorge.no/datasett. - Ved bruk av kart, geodata og stedfestet informasjon i løsningen skal det benyttes karttjenester som er tilgjengeliggjort. Dette sikrer oppdaterte data som er synkronisert med offentlige registre, matrikkel, navn, kretsdata m.m. Ved adressesøk, eiendomssøk, eiersøk skal det offisielle matrikkeltjenestene benyttes
FK-6.1.2	Bakgrunnskart	For visning av egne kartdata skal det benyttes karttjenester levert av av Trondheim kommune og Norge digitalt samarbeidet
FK-6.1.3	Karklient	Kartklient for stedfestet informasjon - Ved søk, oppslag og visning av stedfestet informasjon fra arkiv, fagsystemer e.l. skal det velges en kartklient som støtter tjenester (web services) definert i geointegrasjonsstandarden ver. 1.1 (utvidet) og nye NOARK 5 tjenester
FK-6.1.4	Støtte for formater i kartklient	Kartklienten skal støtte geodatakilder som er definert gjennom Open Geospatial Consortium (OGC): Web Mapping Service (WMS), Web Map Tile Service (WMTS), Web Coverage Service (WCS) og Web Feature Service (WFS). Dersom det ønskes oppdatering av geografiske objekter via web må klienten også støtte WFS-T (Web Feature Service transactional).
FK-6.1.5	Lagring av data inklusive geometri	I tillegg til øvrige datatyper som en database håndterer må databasen ha støtte for datatypen geometri. Geometri er en datatype som benyttes av tjenestelaget for å presentere objektene i visningsklienten
FK-6.1.6	Entydige nøkler for stedfestetinformasjon	Ved behov for lagring av f.eks. adressen i løsningen bør det beholdes entydige nøkler slik at adressen er definert likt på tvers av systemer slik at informasjon mellom tjenestene håndteres likt.
Produktkvalitet		
KK-1.1.1	Funksjonell egnethet	Bruker skal beholde dyplenke og kontekst gjennom autentisering
KK-1.1.2	Funksjonell egnethet	Tjenester i løsningen skal kunne levere dynamiske dyplenker
KK-1.2.4	Funksjonell egnethet	Alle sider skal være uten store kodefeil.
KK-1.3.2	Funksjonell egnethet	Løsningen er utformet slik at kontaktinformasjon er lett tilgjengelig
KK-1.3.3	Funksjonell egnethet	Ved innsending av skjema (fullført transaksjon e.l.) skal løsningen umiddelbart gi en skjermkvittering, eller annen likeverdig respons som bekrefter innsendingen, med informasjon om hvor man kan gjenfinne sin sak og hvor eventuell kvittering er sendt (for eksempel e-postmottaker).
KK-2.2.1	Ytelse	Responstidskrav ved vanlige brukeraktivitet - Ytelse og responstid må være så god at det ikke oppleves ventetid i de vanlige oppgaver. Ventetid skal ikke aksepteres i vanlige lese og registreringsbilder. Innhenting av skjermbilde skal skje uten at en venter mer enn 3 sekund
KK-3.3.1	Pålitelighet	Løsningen må kunne gjenopprette data som er produsert før en ikke planlagt nedetid.
KK-4.1.1	Informasjonsforvaltning	Data i løsningen (eller backup) skal persistere for xxx måneder (avklares nærmere i samarbeid med leverandør)
KK-5.1.1	Brukskvalitet	Løsningen er tilpasset ulike skjermstørrelser (responsivt design).
KK-5.1.2	Brukskvalitet	Hvis det er nødvendig med ventetid skal det gis en indikator på at løsningen arbeider.
KK-5.2.1	Brukskvalitet	Det kommer klart fram at Trondheim kommune er ansvarlig for løsningen.
KK-5.2.2	Brukskvalitet	Løsningen skal utformes i tråd med Trondheim kommunes grafiske profil. Tilpasninger til profilen gjøres i samråd med Kommunikasjonsenheten. (https://sites.google.com/trondheim.kommune.no/grafiskprofil/start)

Videreutvikling av Aktør- Booking- og Tilskuddsbasen

SSA-O Bilag 1 - Vedlegg B Kravtabell Felles krav til produkt funksjonalitet, produktkvalitet og prosesskrav

Felles krav til produktfunksjonalitet, produktkvalitet og prosess		
KravNr.	**Kravområde**	**Krav til løsning**
KK-6.1.2	Sikkerhet	Alle grensesnitt skal validere data ift. lovlig innhold, lengde, ondsinnet innhold mv. Valideringen skal sikre systemene mot trusler som SQL/Command injection, cross-site-scripting osv. Valideringen skal gjelde både eksternt eksponerte grensesnitt (websider/skjema/brukerinput) og bakenforliggende grensesnitt (tjenestekall, databasekall mv.) Det skal benyttes mekanismer som beskytter mot Cross site scripting (XSS), Cross site request forgery (CSRF) og lignende angrep.
KK-6.1.3	Sikkerhet	All kommunikasjon med Løsningen og mellom komponenter i Løsningen skal foregå over krypterte kanaler, og det skal være mulig å blokkere eventuelle usikre/ukrypterte kommunikasjonsporter. Det skal benyttes anerkjente krypteringsmekanismer uten kjente sårbarheter.
KK-6.1.4	Sikkerhet	Løsningen skal beskytte mot kapring av forbindelser mellom lag i løsningen (nettleser/webserver, nettleser/api, webserver/api, webserver/database osv). Autentiseringsnøkler (passord og lignende) skal overføres og lagres på sikre måter, og beskyttes mot brute force gjetting, valideres av alle lag, ikke eksponeres i URL'er, utløpe etter definerte kriterier). Kriterer som OWASP Application security verification standard skal legges til grunn.
KK-6.1.5	Sikkerhet	Alle tjenester som benytter SSL-sertifikater skal benytte offentlige sertifikater med god dekning i standard nettlesere, og uten kjente svakheter. Validering vha. SSL Labs minimum karakter A kan benyttes for å validere oppfyllelse. Alle tjenester som konsumerer andre SSL-baserte tjenester skal validere sertifikater mot et tiltrodd tillitsanker.
KK-6.1.6	Sikkerhet	Løsningen skal leveres med en default sikker konfigurasjon. Komponenter som løsningen bygger på skal ikke ha kjente sårbarheter, unødvendige funksjoner skal være avslått (porter, tjenester, kontoer, rettigheter), default kontoer og tilganger skal være deaktivert, feilmeldinger skal ikke gi unødvendig informasjon til sluttbruker, og servere og rammeverk skal være konfigurert iht. gjeldende sikkerhetsanbefalinger.
KK-6.1.7	Sikkerhet	Ved bruk av elektronisk signering (alternativt forsegling) må denne kontrolleres før elektonisk overføring aksepteres.
KK-6.1.8	Sikkerhet	For løsninger som skal sende ut epost med avsenderadresse under Trondheim kommunes domenenavn, skal utsendelsen primært foregå via Trondheim kommunes epostløsning. Om løsningen sender epost fra egen server, skal denne ha ip som kan registreres i TKs SPF-record og støtte DKIM signering.
KK-6.2.1	Sikkerhet	Løsningen skal levere innhold til audit-log for all bruk av løsningen. Loggen skal inneholde innslag for autentisering, autorisasjon, tildeling og bruk av tilganger, endring av konfigurasjon, systemstart/stop samt oppgraderinger.
KK-6.2.6	Sikkerhet	Logger skal inneholde: Id for bruker Type hendelse Dato og tidspunkt Suksess eller feil Opphav til hendelsen (system/bruker mv.) Identitet eller navn på påvirket data, systemkomponent eller ressurs. Loggdata skal være strukturert på formater og protokoller som muliggjør innsamling til SIEM-løsning/loggkorreleringsløsninger.
KK-6.3.1	Sikkerhet	Ved behov for ikke-benektelse (elektronisk signatur, avtaleinngåelser, inngåelse av forpliktelser), skal ID-portens signaturportal benyttes.
KK-6.4.2	Sikkerhet	Det skal være mulig å endre knytningen mellom roller og rettigheter i løsningen. Alle endringer i rettigheter skal kunne spores i audit-log. Det skal kreves spesielle roller for å endre roller og rettigheter. Endringer skal kunne gjøres uten at systemet restartes
KK-6.4.3	Sikkerhet	Løsningen skal ha støtte for standard roller som systemadministrator, brukeradministrator, system/konfigurasjonsrevisjon, revisjon av logger samt de nødvendige funksjonelle roller <PROSJEKTETS DEFINISJON AV ROLLER I PROSJEKTSPESIFIKKE KRAV> Det skal opprettes hensiktsmessige tilgangsgrupper for brukere for å oppnå effektiv administrasjon av tilganger. Tilganger skal kunne begrenses til ulike geografiske områder og funksjoner (lese, skrive, endre, slette), eventuelt begrenses i forhold til andre krav til dataavgrensning. Tilgang skal kunne variere ut fra klassifisering av informasjon, habilitet, tjenestedeling og ulike typer av tjenstlig behov. Prinsippet om tjenestedeling skal benyttes for å hindre at en medarbeider urettmessig legger inn eller endrer data for egen eller andres vinning. Tilganger til personer med strengt fortrolig adresse (Kode-6) og Fortrolig adresse (Kode-7) skal gis separat

Videreutvikling av Aktør- Booking- og Tilskuddsbasen

SSA-O Bilag 1 - Vedlegg B Kravtabell Felles krav til produkt funksjonalitet, produktkvalitet og prosesskrav

Felles krav til produktfunksjonalitet, produktkvalitet og prosess		
KravNr.	**Kravområde**	**Krav til løsning**
KK-6.5.2	Sikkerhet	Løsningen skal støtte webbaserte API'er for brukeradministrasjon og administrasjon av tilganger. API'ene skal kunne gjøre det mulig å opprette/slette brukere, flytte brukere mellom organisasjonsenheter, roller og grupper fra en ekstern IAM-løsning. (Automatisering av brukeradministrasjon)
KK-6.5.3	Sikkerhet	ID-Porten skal benyttes for autentisering av eksterne brukere ("publikum") når det er behov for entydig identifisering. (krav ved bruk av ID-porten, se Felles produksjonsfunksjonalitet)
KK-6.5.5	Sikkerhet	For autentisering mot applikasjoner og tjenester som gir tilgang til informasjon på sikkerhetsnivå 3 eller 4, eller for handlinger som kan ha betydelig økonomisk eller sikkerhetsmessig påvirkning for Trondheim kommune, skal det kreves sterk autentisering/2-faktor autentisering.
KK-6.5.8	Sikkerhet	Løsningene skal støtte single-sign-on og single-log-off innenfor samme autentiseringsmekanisme og sikkerhetsnivå. Det skal implementeres timeoutmekanismer som krever reautentisering etter <XX> minutter inaktivitet (avklares nærmere med leverandør). Løsningen skal støtte at tjenesten krever reautentisering (bryte single-signon/force reauthentication).
KK-6.5.10	Sikkerhet	Løsningen skal validere tilgangsrettigheter i alle lag av applikasjonen, og validere at brukeridentiteten som aksesserer data eller tjenester har nødvendige rettigheter. Valideringen skal ikke kunne omgås av brukeren.
KK-7.1.1	Vedlikeholdbarhet	Løsningen må være bygd opp av uavhengige komponenter som enkelt kan byttes eller oppgraderes med minimale konsekvenser for andre komponenter.
KK-7.3.1	Vedlikeholdbarhet	Løsningen skal logge feil, transaksjoner, brukmønster, dataflyt og gjøre logger tilgjengelig slik at analyse av løsningen for forbedring blir mulig.
KK-7.5.1	Vedlikeholdbarhet	Leverandøren må tilgjengeligjøre testverktøy slik at kunden har muligheten til å etterprøve krav til bl.a ytelse og sikkerhet.
KK-8.1.1	Kompatibilitet	Tjenester skal som hovedregel tilbys som web services, enten som REST-API eller SOAP-basert.
KK-8.1.2	Kompatibilitet	Meldingsstruktur skal følge standard protokokoler som JSON, XML eller ATOM.
KK-8.1.3	Kompatibilitet	Løsningen skal benytte fag standard protokoller: Noark5 WS- eller Geointegrasjonsgrensesnitt (GI) for opprettelse, overføring og oppdatering av arkivobjekter FHIR eller SCAIP for helse løsninger.
KK-8.1.4	Kompatibilitet	Tjenester som tilbys må versjoneres. Der det er nødvendig må det tilbys multi-versjonshåndtering i eksponerte grensesnitt.
KK-8.1.5	Kompatibilitet	WSI-profiler - SOAP/XML tjenester skal være WSI- kompatible.
KK-8.1.6	Kompatibilitet	Webbaserte APIer skal dokumenteres blant annet med, men ikke begrenset til, WSDL, WADL eller Swagger. Dette innebærer at mal for API informasjonen skal fylles ut og holdes oppdatert: https://docs.google.com/spreadsheets/d/1GhpmOi1w8oI73i4k7ebnY2zM5UjuwfT3DR08_TfgCH4/edit#gid=23894008
KK-9.1.1	Portabilitet	All funksjonalitet må være tilgjengelig ved bruk de vanligste nettlesere (Chrome, Firefox, Safari, IE/Edge)
KK-9.1.2	Portabilitet	All funksjonalitet må være tilgjengelig ved bruk på PC, mobil og nettbrett.
Prosesskrav		
PK-1.1.1	Sikker utvikling	Leverandør skal gjennomføre sikkerhetstester i henhold til anerkjente retningslinjer for sikkerhetstesting, som OWASP Application Security Verification Standard (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project).
PK-1.1.2	Sikker utvikling	Leverandøren skal sikre og dokumentere at alle utviklere har nødvendig kunnskap om sikker programvareutvikling, og gjennomføre nødvendige bakgrunnssjekk av eget personell.
PK-1.1.3	Sikker utvikling	Leverandøren skal benytte et kildekontrollsystem som autentiserer opphavet til og logger alle endringer i kildekoden og konfigurasjonsfiler.
PK-1.1.4	Sikker utvikling	Leverandøren skal holde kontroll med all tredjeparts biblioteker og komponenter i løsningen for avdekkede sikkerhetssårbarheter og oppdateringer som har betydning for løsningen, og sørge for at feil i tredjepartsbibliotek som innebærer behov for feilretting av løsningen leveres under samme vilkår som feilrettinger i egenutviklede komponenter.

Videreutvikling av Aktør- Booking- og Tilskuddsbasen

SSA-O Bilag 1 - Vedlegg B Kravtabell Felles krav til produkt funksjonalitet, produktkvalitet og prosesskrav

Felles krav til produktfunksjonalitet, produktkvalitet og prosess		
KravNr.	**Kravområde**	**Krav til løsning**
PK-1.1.6	Sikker utvikling	Leverandøren skal utarbeide en løsningsbeskrivelse for sikkerhet som beskriver hvordan Leveransen oppfyller krav til: Inputvalidering Autentisering og sesjonshåndtering Tilgangskontroll, roller og rettigheter Feilhåndtering Logging Sikring av forbindelser til eksterne system og mellom de ulike løsningskomponenter. Kryptering og konfidensialitetssikring Tilgjengelighet og sikring mot datatap Sikker konfigurasjon og Generelle sårbarheter, inkl. beskyttelse mot vanlige feil som «OWASP Top Ten Most Critical Web Application Vulnerabilities» Der Leverandørens løsningsbeskrivelse forutsetter at sikkerhetsfunksjoner ivaretas av komponenter som ikke er en del av den leverte løsningen, skal dette dokumenteres spesifikt i løsningsbeskrivelsen. Løsningsbeskrivelsen skal godkjennes av Kunden.
PK-1.1.9	Sikker utvikling	Leverandøren skal sikre at identifiserbare personopplysninger ikke benyttes i testmiljø eller verifikasjonsmiljø som ikke har tilsvarende tilganger som produksjonstjenesten.
PK-1.2.2	Driftssikkerhet	Sikkerhetsrevisjon Kunden, eller tredjepart av kunden, skal kunne gjennomføre revisjon av sikkerheten i løsningen. Krav til revisjon kan også oppfylles ved uavhengig tredjeparts revisjon av tjenesten iht. ISO 27001 eller tilsvarende. Dokumentasjon av gjennomført tredjeparts revisjon skal kunne forevises Kunden.
PK-1.2.3	Driftssikkerhet	Krav til databehandleravtale Leverandøren skal inngå skriftlig databehandleravtale med Kunden. Hvis Leverandørens tjenesteleveranse omfatter overføring av personopplysninger til tredjeland som ikke har tilstrekkelig databeskyttelse iht. EUs personverndirektiv, skal databehandler inngå databehandleravtale iht. EU Commission Decision C(2010)593 Standard Contractual Clauses (processors) og implementere de sikkerhetstiltak som er nødvendige for å etterleve EUs personverndirektiv.
PK-1.2.5	Driftssikkerhet	Gjenopprettingstid etter at nødvendig infrastruktur er gjenskapt Avhengig av klassifisering av tilgjengjelighet skal systemene kunne gjenskapes epå en gitt tid etter at infrastruktur og systemprogrammer fungerer som normalt: MIDDELS 10 timer HØYT 6 timer EKSTRA HØYT 2 timer
PK-1.2.6	Driftssikkerhet	Krav til sikkerhetskopiering Sikkerhetskopier skal sikre mot tap av informasjon som følger av feil i utstyr og programmer eller av feilaktig operering og bruk. Klassifisering angir når sikkerhetskopi skal tas: LAV - En gang pr. uke MODERAT - Før batchkjøringer + Daglig endringskopi MIDDELS og høyere - Før og etter transaksjoner til bruk ved tilbakerulling.
PK-1.2.8	Driftssikkerhet	Krav til gjenskapingsmuligheter Det må finnes systemer, rutiner og instrukser for å gjenskape tapt informasjon best mulig på grunnlag av sikkerhetskopier og beredskapskopier. Ved gjenskaping av data ("recovery") må det sikres at de sammenhenger som skal være oppfylt mellom data blir oppfylt (konsistens må sikres).