

Bilag til SSA-L
Bilag 1: Kundens kravspesifikasjon
Kjøp av nye kart- og forvaltningsløsninger for geodata
Del II - Sikkerhetskrav

Sikkerhetskrav

Krav Nr.	Forventninger til tjenesten	Krav-type	Vekting av krav
S-1	Rammeverk for kontrolltiltak Leverandørkjeden skal være sikret med kontrolltiltak for informasjonssikkerhet gjennom rammeverk som er standardisert. Løsningsbeskrivelse Rammeverket skal være tilsvarende ISO 27001/27002, ISF SOGP, COBIT, Common Criteria, CSA CCM e.l. Leverandørene bes vise til eventuell gyldig sertifisering og beskrive hvilke kontrolltiltak som er benyttet. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver sin løsning	A	N/A
S-2	Standardisert sikkerhetsstyring Leverandøren skal alltid benytte et sikkerhetsstyringssystem som er anerkjent, standardisert og som periodisk er underlagt revisjon av autorisert tredjepart for godkjenning eller sertifisering. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-3	Leverandør skal levere revidert sikkerhetsrapport Leverandører skal på forespørsel fra Plan- og Bygningsetaten alltid tillate og legge til rette for revisjon av systemer, sikkerhetsstyring og driftsmiljø som er del av leveransen eller brukes i leveransen. Revisjonen skal kunne utføres av Plan- og Bygningsetaten eller leverandøren skal kunne fremlegge en rapport fra en uavhengig tredjepart som er lisensiert og anerkjent av standardiseringsorganisasjon. Rapporten skal være i henhold til internasjonalt anerkjent standardisert sikkerhetsgjennomgang godkjent av standardiseringsorganisasjonen. Rapporten skal ikke være eldre enn 12 måneder. Eksempelvis kan en slik rapport være en SOC-2.	A	N/A

	<u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».		
S-4	Diskresjon om kundeinformasjon Leverandører skal alltid konsultere og få skriftlig eksplisitt aksept fra Plan- og Bygningsetaten før de deler informasjon med andre eller benytter til KI/ML som omhandler Plan- og Bygningsetatens kundeforhold, behov, innsikter, operasjonell bruk, metrikker eller måledata ved bruk av løsninger, eller annen informasjon gitt leverandør gjennom kommunikasjon med Plan- og Bygningsetaten. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-5	Beskytte selvbetjente oppdateringer Leverandører skal alltid formidle enhver oppdatering til løsninger for Plan- og Bygningsetaten gjennom forsvarlig kryptert forbindelse. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-6	Løsninger utviklet med sikkerhetsprinsipper Leverandøren bør kunne redegjøre for hvordan de følger og bruker prinsippene for Security by Design og Privacy by Design (innebygd personvern) <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	0,5
S-7	Separerte utviklingsmiljøer Leverandør bør kort vise til hvordan løsninger som tas i bruk benytter separate miljøer for utvikling, testing og produksjon. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	0,5

S-8	Sikkerhet som del av løsnings livsløp Leverandør bør kort vise til hvordan sikkerhet ivaretas som del av løsningenes livsløp (S-SDLC, DevSecOps). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-9	Testing del av dataflyters livsløp Enhver løsning som tas i bruk skal alltid testes slik at den aldri vil tillate direkte dataflyt til eksternt eksponerte systemer fra interne systemer for innhold, men skal alltid ha et system for tilstrekkelig kontroll på dataflyt mellom disse (dvs minimere angrepsflater, lekkasjemulighet). <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-10	Testing av AppSec Leverandør som benytter web-protokoller i sin løsning, bør beskrive hvordan testing for nyeste offisielle OWASP Top 10 for applikasjonssikkerhet utføres og er del av livsløpet. Web-protokoller er enhver protokoll som HTTPS, HTTP, WebSocket, WebRTC m.v der en nettleser kan benyttes som klient eller der en ressurs i bruk av en løsning kan angis med en URI (enhver W3C/IETF Uniform Resource Identifier dvs. også semantisk datamodellering). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-11	Testing av APler Leverandør bør beskrive hvordan testing for nyeste offisielle OWASP API Security Top 10 utføres og er del av livsløpet når løsningen mottar via APler. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-12	Sikring mot kjente sårbarhetstyper	B	1

	Leverandøren bør kort viste til hvordan løsninger som tas i bruk testes og sikres mot sårbarhetstyper angitt i CWE utføres og er del av livsløpet. CWE står for "Common Weakness Enumeration". <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.		
S-13	Vise kjente sårbarheter Leverandøren bør kort beskrive alle kjente sårbarheter og alle kjente feil i løsningen. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-14	Kontroll mot kjente sårbarheter Leverandøren bør kort beskrive hvordan løsninger som tas i bruk kontrollerer avhengigheter og komponenter mot CVE-database som del av livsløpet, og alltid tidfester dato for når første kontroll ble foretatt og hvor ofte kontroll er gjort siden. Kildene til CVE-databasene skal alltid navngis, kort beskrives og siste oppføring i databasene som benyttet for kontroll av løsningene skal alltid angis sammen med sin offisielle unike referanse. CVE står for "Common Vulnerabilities and Exposures" og er et internasjonalt søkbart referansesystem for kjente sårbarheter, og SBOM, CBOM m.v. er metoder for dette. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-15	Kartlegge sikkerhetssensitiv kode Leverandøren bør kort beskrive og kartlegge alle deler, moduler, komponenter og områder i løsningen som inneholder sikkerhetssensitiv kode og funksjonalitet. Sikkerhetssensitivitet er håndtering av passord, pålogging, autentisering, autorisering, kryptering, informasjonssikring (konfidensialitet, integritet, tilgjengelighet), sporbarhet i nettverkskommunikasjon og formidling av logger. Kartleggingen bør alltid være et visuelt diagram. Beskrivelsene bør alltid være gitt som tekst, og helst i tabellform med referanser til diagram-deler. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1

S-16	Risikobasert leverandørtilgang For at en leverandør og underleverandør skal kunne gis utvidede behovsbaserte rettigheter må det foreligge en godkjent risikovurdering. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-17	Risikobasert datamigrering Leverandører kan ikke flytte eller kopiere data ut eller inn fra IKT-utstyr i Plan- og Bygningsetatens nettverk, uten at det foreligger en godkjent risikovurdering. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-18	Isolering ved tilgang Når leverandører gis tilgang skal det etableres tekniske barrierer som hindrer leverandøren i å få tilgang til annet enn hva som er formålet med tilgangen. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-19	Databehandlingens opphør Ved opphør av kontrakt plikter leverandør å følge instruks for terminering som beskrevet i databehandleravtale. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-20	Høyrisikoland vurderes Det skal eksplisitt fremkomme i risikovurderingen om leverandøren benytter eller er avhengig av produksjon eller tilgang, i eller fra høyrisikoland (jf. NSM og PST). <u>Utformingskrav</u>	A	N/A

	Leverandøren besvarer kravet med «lest og akseptert».		
S-21	Lovmessig databehandling Leverandør og underleverandør skal bekrefte at de er kjent med og etterlever kravene i personopplysningsloven/GDPR. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-22	Databehandling i tredjeland Kundedata skal lagres og behandles innenfor EU/EØS. Leverandøren skal ikke overføre kundedata til land utenfor EU/EØS uten oppdragsgivers forhåndsgodkjenning <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-23	Løsninger jf. føringer Utforming, drift, bruk og administrasjon av informasjonssystemer samstemmer med aktuelle lover, forskrifter og kontraktsfestede krav til sikring. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-24	Systemet støttes i hele levetiden Systemet med underliggende komponenter skal supporteres i kontraktsperiodens levetid. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-25	Sikre produksjonsdata Plan- og Bygningsetatens produksjonsdata skal ikke benyttes i eller kopieres til andre miljøer, eksempelvis for test eller utvikling av andre tjenester uten skriftlig eksplisitt avtale med Plan- og Bygningsetaten.	A	N/A

	<u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».		
S-26	Eierskap til data Data som lagres skal forbli i Plan- og Bygningsetaten sitt eierskap, og Plan- og Bygningsetaten beholder eierskapet til data også etter at kontrakten er terminert. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-27	Innsyn og deling av data Data skal ikke eksporteres til andre parter eller leverandører uten skriftlig eksplisitt avtale med Plan- og Bygningsetaten. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-28	Leverandør skal inngå taushetserklæring Alle leverandører som tar del i leveransen, skal alltid undertegne Plan- og Bygningsetaten sin gjeldende taushetserklæring. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-29	Fortrolig håndtering av data Leverandør skal ikke dele Plan- og Bygningsetatens data med tredjepart eller underleverandør (inkludert via KI/ML modellering) uten at dette på forhånd er skriftlig eksplisitt godkjent av Plan- og Bygningsetaten. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-30	Fortrolighet om avlede data	A	N/A

	Leverandør skal aldri dele eller overføre logger som tilhører, vedrører eller som kan avsløre Plan- og Bygningsetaten til noen andre kunder. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».		
S-31	Planlegge skalering for bruk av APler Hvis leverandøren har løsninger som benytter APler for deling eksternt, skal leverandøren kartlegge forventede brukere med forventet dataflyt, hyppighet og trafikkmengde ved oppstart og ved full produksjon slik at tilgjengelighet og stabilitet kan planlegges for driftsløsning og sikkerhet. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver sin løsning	A	N/A
S-32	Robust identitetskontroll Alle kontoer skal entydig knyttes opp mot en digital identitet, og ivareta kravene om uavviselighet og sporbarhet ved autentisering. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-33	Robuste privilegerte tilganger Bruk av privilegerte tilganger i systemer i Plan- og Bygningsetaten er uavviselig. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-34	Herding og minimalisert konfigurasjon Leverandør skal alltid sette minimal konfigurasjon av løsningen tilpasset Plan- og bygningsetatens behov for ethvert system og funksjon, og herding etter beste praksis og gjerne nyeste CIS Benchmark. <u>Utformingskrav</u>	A	N/A

	Leverandøren besvarer kravet med «lest og akseptert» og beskriver herdingen.		
S-35	Endre alle standardpassord Absolutt alle standardpassord og pre-konfigurerte tilganger skal endres, informeres om og tilpasses unikt for Plan- og bygningsetaten før løsninger tas i bruk. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-36	Prinsipp for logging Alle relevante handlinger skal logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges: Alle typer innlogginger, inkl. forsøk på innlogginger; Oppretting, endring og sletting av informasjonsobjekter; Oppretting, endring og sletting av andre brukere; Innsyn eller endring i personopplysninger; Endringer, eller forsøk på endringer, i systemkonfigurasjonen. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-37	Risikobasert avgrenset tilgangsstyring Leverandør skal alltid begrense og kontrollere tilganger til løsningen fra alle lokasjoner og klienter basert på risiko. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort hvordan.	A	N/A
S-38	Samlet kontroll over APIer Løsninger som benytter APIer for deling eksternt bør benytte felles kontrollmekanismer og sikkerhetstjenester som gir en samlet kontroll over dataflyt i, til og fra løsningen. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning. Beskriv utfyllende hvordan med diagram og tekstbeskrivelse som understøtter diagram.	B	0,5

S-39	Verifisere dataflyt og konfigurasjon Leverandør bør automatisk og periodisk verifisere faktisk dataflyt og effektiv konfigurasjon for dataflyt av løsningen. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	0,5
S-40	Kontrollere dataflyt for APler Leverandøren skal sikre at løsninger som eksponeres via APler utelukkende tilgjengeliggjøres bak felles løsning for kontroll over dataflyt som API-gateway. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort etterlevelsen	A	N/A
S-41	Begrenset publisasjon av APler APler for deling eksternt skal aldri publiseres eller tilkjennegjøres utenfor Plan- og bygningsetaten før nødvendige sikkerhetstiltak og full etterlevelse foreligger, samt forsikring om at dataflyt til og fra APler går gjennom etablerte sikkerhetsmekanismer. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort etterlevelsen.	A	N/A
S-42	Kontroll på datatrafikk APler for deling eksternt skal alltid godkjennes skriftlig av oppdragsgiver. Det må være mulig å identifisere brukergrupper. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort etterlevelse	A	N/A
S-43	Unngå og forhindre peer-to-peer	B	0,5

	Leverandør bør unngå, forhindre og ellers minimere direkte kommunikasjon mellom klienter i løsninger som tas i bruk. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.		
S-44	Beskytt bakenforliggende systemer Leverandør bør minimere eksponering av bakenforliggende systemer og deres data, spesielt ved mottak via APler, for løsningene. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	0,5
S-45	Tillat aldri direkte dataflyter til eksterne Enhver løsning som tas i bruk skal aldri tillate direkte dataflyt til eksternt eksponerte systemer fra interne systemer for innhold, men skal alltid ha et system for tilstrekkelig kontroll på dataflyt mellom disse. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort etterlevelsen.	A	N/A
S-46	Forhindre direkte dataflyt til kritisk system Løsninger som tas i bruk bør alltid forhindre direkte dataflyt fra eksponerte systemer til andre interne kritiske systemer. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-47	Gjenbruk identiteter Løsninger som tas i bruk skal bruke identiteter som er autentisert og autorisert, og med Plan- og Bygningsetatens standard (Entra-ID). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	A	N/A

S-48	Bruk single-sign-on Løsninger som tas i bruk skal støtte Plan- og Bygningsetaten sine systemer for single-sign-on eller tilsvarende. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	A	N/A
S-49	Brukerkontoer og fellesenheter Det skal kun benyttes personlige brukere. Fellesbrukere eller på annen måte deling av brukerkontoer skal ikke forekomme. Dette gjelder ikke fullt administrerte mobile enheter med flere brukere. Informasjonstilgang styres gjennom apper som vil knyttes til personlig bruker-ID, men operativsystemet kan ikke skille brukere. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-50	Fødererert autentisering Tjenester som skal ha tilgang til autentiseringsmetoder skal benytte seg av standardiserte fødereringsprotokoller mot sentral autentiseringstjeneste. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-51	Driftskontoer sikres PAM skal benyttes for alle ikke-personlige kontoer som service- og administratorkontoer. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-52	Drift via servicekontoer Regelmessige og planlagte oppgaver på IKT-systemene skal kjøres av servicekontoer. Servicekontoer skal standardiseres og herdes iht. herding av systemer og tjenester. <u>Utformingskrav</u>	A	N/A

	Leverandøren besvarer kravet med «lest og akseptert».		
S-53	Personlige brukerkontoer Brukerkontoer skal ikke gis administrative rettigheter. For behovsbaserte formål skal separate personlige kontoer med utvidede rettigheter opprettes. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-54	Rollebasert tilgang Tilganger skal være basert på rollestyring. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-55	Tilgang til personopplysninger Tilganger til personopplysninger skal begrenses til behov knyttet til brukerens roller og organisasjonstilhørighet. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-56	Gyldig grunnlag for tilgang Privilegerte tilganger tildeles kun når det foreligger gyldig grunnlag for databehandling. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-57	Tilgang ved tjenstlig behov Privilegerte tilganger tildeles kun i henhold til tjenstlig og dokumentert behov. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A

S-58	Sikkerhetskontroll av innhold Løsninger som tas i bruk bør sikkerhetskontrollere data som presenteres eller formidles til brukere av Plan- og Bygningsetatens systemer (sikret integritet). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-59	All mottakelse krypteres Løsninger som tas i bruk bør benytte kryptering for mottak via APler og eksterne koblinger. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-60	Kryptering av lagringsmedium Alle lagringsmedium for operasjonelle data og analytiske data skal være kryptert med styrke og metoder som beskrevet i gjeldende krypteringsanbefalinger fra NSM, eller med bedre styrke som i så fall skal beskrives ytterligere med minst samme detaljnivå som i NSM sine gjeldende krypteringsanbefalinger. Dette omfatter lagringsmedium som inneholder data i bruk av konfigurasjon, applikasjon og infrastruktur, samt alle data som avledes av disse. Lagringsmedium er alle faste installerte samt virtuelle og mobile lagringsmedium. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-61	Kryptering av data i ro og transitt Løsningen skal kryptografisk signere alle sensitive operasjonelle data som overføres mellom systemer, separate komponenter, over grensesnitt eller fra skytjenesten etter gjeldende krypteringsanbefalinger fra NSM. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-62	Kryptering og krypteringsnøkler	B	1

	Leverandør bes beskrive støttede eierskapsmodeller og beskyttelsesregime samt utstedere (CAer) Plan- og Bygningsetaten kan benytte for krypteringsnøkler som skal brukes i løsningen. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.		
S-63	Varsling av endringer relatert til krypteringsprosedyrer Leverandør bes beskrive hvordan de vil rapportere alle betydelige endringer relatert til krypteringsprosedyrer (endringer av nøkkellengde, algoritmer eller prosedyrer for nøkkelhåndtering etc). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-64	Sikkerhetskopier alt Leverandøren bør automatisk og jevnlig sikkerhetskopierte alt innhold, konfigurasjon, systemoppsett og installasjon av løsninger <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-65	Test sikkerhetskopier Leverandøren bør jevnlig teste at gjenopprettet sikkerhetskopi for Plan- og Bygningsetaten kan erstatte løsningene. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-66	Sikre datahåndtering hos tredjepart Hvis sikkerhetskopier av data tilhørende eller vedrørende Plan- og Bygningsetaten oppbevares eksternt hos partner eller tredjepart må leverandør vise til avtale og hvordan tredjepart sikrer dataene. Ved personopplysninger må en databehandleravtale alltid inngås i forkant. <u>Utformingskrav</u>	A	N/A

	Leverandøren besvarer kravet med «lest og akseptert».		
S-67	Forespørsel om sletting Beskriv tiden leverandøren behøver for å slette data og alle kopier av data etter at det har blitt forespurt eller bestilt av Plan- og Bygningsetaten. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-68	Leverandør skal bruke sikker metode for sletting av data Leverandøren skal alltid benytte sikre metoder for sletting av data på fysiske medium og ha etablert slike rutiner ved avslutning av levetiden for medium. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert» og beskriver kort metoder og rutiner for dette.	A	N/A
S-69	Automatisk overvåking Leverandøren bør ha automatisk overvåking med varsling av løsninger som tas i bruk og jevnlig kartlegge disse for sårbarheter gjennom hele livsløpet (inkludert utvikling). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-70	Sentralisert automatisk sikring Løsninger som tas i bruk bør beskyttes med sentralisert automatisk sikring mot trusler og sårbarheter (f.eks. IDS, IPS, SOAR, SASE, CASB). <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-71	Kvalitetskontroll av sporingsmekanismer	B	1

	Leverandøren bør automatisk jevnlig forsikre at kvalitet på registrerte logger og hendelser for løsninger ikke forringes og er korrekt. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.		
S-72	Beskyttelse av sporingsmekanismer Løsninger som tas i bruk bør beskytte konfidensialitet, integritet og tilgjengelighet til logger og registrerte hendelser. <u>Utformingskrav</u> Leverandøren besvarer kravet med "J" eller "N". Ved "J" beskriver leverandøren sin løsning.	B	1
S-73	Synkronisert tidsangivelse Løsninger som tas i bruk skal alltid benytte samme tidskilde (for klokkefunksjon, viktig for krypteringsfunksjoner og sporbarhet) i alle komponenter. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-74	Standardisert logging Alle IKT-systemer skal logge hendelser i et standardisert format. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-75	Tilgang på logger Alle IKT-systemene skal tilgjengeliggjøre logger for gjennomgang og eksport. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A
S-76	Sentralisert sikkerhetslogging	A	N/A

	Logger som er relevante for informasjonssikkerheten skal kunne overføres til sentralt loggmottak. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».		
S-77	Tidskilde til logger Logger skal ha tidsstempling og klokken benyttet til tidsstemplingen skal være synkronisert mot sentral tidskilde (NTP-tjeneste). <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-78	Kravstyrt oppbevaring av logging Logger skal oppbevares i tråd med krav. Som minimum gjelder 24 måneders lagring for sikkerhetslogger, lagring utover dette må spesifiseres i avtale. For journallogger eller andre logger knyttet til saksbehandlingsrettede registre, gjelder egne krav. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-79	Loggføre tilgangskontroll Tilganger skal loggføres. I tillegg skal endringer i tilganger og hvem som beslutter endringer i disse også loggføres. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-80	Behandling av logger Logger skal kunne gjennomgå manuelt eller automatisk basert på forhåndsdefinerte kriterier. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert»	A	N/A

S-81	Varsle om forhold som påvirker lovkrav Leverandør skal alltid varsle Plan- og Bygningsetaten uten opphold om forhold som vil kunne påvirke Plan- og Bygningsetatens eksisterende eller forestående lovkrav. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A
S-82	Varsle om endring i tjenestelokasjon Leverandør skal alltid rapportere innen rimelig tid om endringer av geografisk lokasjon for tjenesten til Plan- og Bygningsetaten slik at det gis praktisk mulighet for innspill eller innsigelser. <u>Utformingskrav</u> Leverandøren besvarer kravet med «lest og akseptert».	A	N/A