Sikkerhedsbilag

1. Indledning

1.1 Sikkerhedsbilaget er et bilag til [KONTRAKT].
1.2 Sikkerhedskravene i sikkerhedsbilaget er udformet på basis af anerkendte standarder som, ISO 27001 og SANS CIS.
1.3 Sikkerhedsbilaget skal ses i sammenhæng med en eventuel Databehandleraftale, således at de databeskyttelsesmæssige forpligtelser som følger af Databeskyttelsesforordningen, og som fremgår af Databehandleraftalen, gælder foruden sikkerhedskravene i sikkerhedsbilaget.

2. Sikkerhedskrav

2.1 Nogle sikkerhedskrav suppleres af en kvalitetsegenskab.
2.2 Kvalitetsegenskaben specificerer det grundlæggende sikkerhedskrav yderligere baseret på Kundens egen risikovurdering af den Ydelse, som Leverandøren foretager på vegne af Kunden.
2.3 Leverandøren skal overholde sikkerhedskravet samt sikkerhedskravets kvalitetsegenskab.

Kontrol-ID	Sikkerhedskrav	Kvalitetsegenskab
Autorisation og adgangsstyring		
KTRL-201	Leverandøren skal fastlægge, dokumentere og vedligeholde politikker for adgangsstyring i relation til Kontraktens opfyldelse i overensstemmelse med den til enhver tid gældende risikovurdering, jf. KTRL-174.	
KTRL-202	Leverandøren skal sikre, at kun de berettigede Brugere, herunder konsulenters, underleverandørers samt Leverandørens egne medarbejdere, har adgang til de data, som er omfattet af Kontrakten.	Leverandøren skal til enhver tid kunne dokumentere, hvem der har adgang til de løsninger som anvendes for at understøtte Ydelsen i Kontrakten.
KTRL-203	Leverandøren skal implementere en formel procedure for registrering og afmelding af Brugere med henblik på tildeling af adgangsrettigheder i forbindelse med Kontraktens opfyldelse.	Leverandøren skal til enhver tid kunne dokumentere proceduren, samt at den overholdes.
KTRL-204	Leverandøren skal implementere en formel procedure for tildeling, ændring og tilbagekaldelse af adgangsrettigheder for alle brugertyper til alle systemer og tjenester, der anvendes til Kontraktens opfyldelse.	Leverandøren skal til enhver tid kunne dokumentere proceduren, samt at den overholdes.

KTRL-205	Leverandøren skal begrænse og styre tildeling og anvendelse af privilegerede adgangsrettigheder i relation til Kontraktens opfyldelse. Rettigheders skal tildeles med udgangspunkt i "Least Privilege".	Styring af priviligerede adgangsrettigheder skal være omfattet af procedurerne i medfør af KTRL-204.
KTRL-207	Leverandøren skal sikre, at Brugere og Brugeres rettigheder, som er relevante ifm. Kontrakten, gennemgås af Leverandøren med jævne mellemrum. Dette gælder alle Brugere, herunder egne, konsulenters og underleverandørers.	Adgangsrettigheder og autorisationer gennemgås minimum 1 gang årligt, og gennemgangen dokumenteres.
KTRL-208	Leverandøren skal have en procedure for at inddrage alle medarbejderes og eksterne brugeres adgangsrettigheder og autorisationer til information og informationsbehandlingsfaciliteter i relation til Kontraktens opfyldelse, når deres ansættelsesforhold, kontrakt eller aftale ophører eller skal tilpasses efter en ændring.	Leverandøren skal til enhver tid kunne dokumentere proceduren, samt at den overholdes.
Compliance		
KTRL-285	Leverandøren skal sikre, at privatlivets fred og personoplysninger i relation til Kontraktens opfyldelse beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter. Hvis der som tillæg til hovedaftalen er vedlagt databehandleraftale ang. persondatabehandling, har den specifikke instruks for persondatabehandling forrang over for eventuelle modstridende krav.	
Informationssikkerhedspolitikker		
KTRL-176	Leverandøren skal fastlægge et sæt politikker for informationssikkerhed i relation til Kontraktens opfyldelse, som skal godkendes af Leverandørens ledelse, offentliggøres og kommunikeres til Leverandørens medarbejdere og eventuelle underleverandører, og som skal indgå i Leverandørens ISMS, jf. KTRL-173, og understøtte den gældende risikovurdering, jf. KTRL-174.	Leverandøren skal på Kundens anmodning kunne dokumentere gældende politikker for Kunden.
KTRL-177	Leverandørens politikker for informationssikkerhed i relation til Kontraktens opfyldelse skal gennemgås med planlagte mellemrum ud fra en risikobaseret tilgang, samt i tilfælde af væsentlige ændringer, herunder i den gældende risikovurdering, for at sikre politikkernes fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	
Interne informationssikkerheds- og databeskyttelsespolitikker		
KTRL-187	Leverandøren skal sikre, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer i relation til Kontraktens opfyldelse, gennem løbende kontroller, som er defineret i Leverandørens ISMS, jf. KTRL-173.	

KTRL-188	Leverandøren skal sikre, at Leverandørens medarbejdere og, hvor det er relevant, underleverandører ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer i det omfang, det er relevant for deres jobfunktion og Kontraktens opfyldelse.	Der skal afholdes ajourføringsforløb for sikkerhedspoliktikker og procedurer for medarbejdere minimum 1 gang årligt.
KTRL-142	Leverandøren skal sikre uddannelse af medarbejdere, så alle nødvendige kompetencer og kvalifikationer er til stede for at gennemføre Kontraktens krav til informationssikkerhed.	Leverandøren skal minimum 1 gang årligt gennemføre en opfølgning på, at kompetencer og kvalifikationer er til stede, fx ved at medarbejderne gennemfører en test omkring generel informationssikkerhed, datahåndtering etc.
KTRL-190	Leverandøren skal sikre, at informationssikkerhedsansvar og -forpligtelser i relation til Kontraktens opfyldelse, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejdere eller kontrahenter samt håndhæves.	
ISMS og risikostyring		
KTRL-173	Leverandøren skal med henblik på løbende sikring af informationssikkerhed i tilknytning til levering af ydelserne opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO27001 eller tilsvarende (national eller international) anerkendt standard baseret på en risikostyringsproces, jf. KTRL-174, og i overensstemmelse med de i KTRL-175 angivne specifikke krav til Leverandørens ISMS. Leverandøren skal herunder løbende tilpasse sit ISMS, såfremt Leverandørens opdatering af sin risikovurdering, jf. KTRL-174, medfører et behov herfor.	

KTRL-174	Leverandørens risikostyring af informationssikkerheden i forhold til Leverandørens opfyldelse af Kontrakten skal baseres på en dokumenteret og regelmæssigt opdateret risikovurdering. Risikovurderingen kan være en sammenfattet risikovurdering eller en kombination af specifikke risikovurderinger af forskellige områder eller tekniske løsninger. . I relation til Leverandørens risikovurdering gælder det, at: • Risikovurderingen skal omfatte de Ydelser og de dele af Leverandørens virksomhed, som kan have konsekvenser for informationssikkerheden og databeskyttelsen af data omfattet af Kontrakten. • Leverandøren skal sikre, at risikovurderingen er opdateret, og at der forelægger en proces for at genbesøge risikovurderingen i forbindelse med forestående ændringer af Leverandørens egne organisatoriske forhold, forestående ændringer af en eventuel underleverandørs forhold eller forestående ændringer af tekniske løsninger, der har konsekvenser for informationssikkerheden og databeskyttelsen med de i Kontrakten forbundne Ydelser, • Leverandøren skal opdatere sin risikovurdering efter påbud fra Kunden om at inkludere en specifik trussel i risikovurderingen, herunder men ikke begrænset til som følge af ændringer i Kundens egen til enhver tid gældende risikovurdering og/eller konsekvensanalyse vedrørende databeskyttelse (DPIA). En sådan af Kunden påbudt opdatering af Leverandørens risikovurdering skal ske inden for en passende frist henset til truslens karakter. • Leverandøren uden ugrundet ophold skal fremsende Leverandørens gældende risikovurdering med henblik på Kundens godkendelse, og således at Kunden til enhver tid har Leverandørens seneste risikovurdering.	
KTRL-175	Leverandøren skal sikre, at Leverandørens ISMS understøtter, at kravene i sikkerhedsbilaget bliver overholdet. Det kan ske ved at sikre, at kontrollerne er etableret i Leverandørens ISMS-årshjul.	
Leverandørstyring		
KTRL-269	Leverandøren skal have procedurer for auditering af sine Leverandører, som sikrer, at eventuelle Underleverandører, der anvendes til Kontraktens opfyldelse, er omfattet af procedurerne. Er der mellem parterne indgået en databehandleraftale, vil forpligtelsen for tilsyn med Underdatabehandlere fremgå heraf..	Gennemgang og auditering af underleverandørydelser skal gennemføres minimum 1 gang årligt.
Mobilt udstyr		
KTRL-183	Leverandøren skal implementere en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr i forbindelse med opfyldelse af Kontrakten.	Leverandørens klienter skal som minimum overholde øvrige relevante krav opstillet i kravkataloget.
Sikkerhed på klienter		

KTRL-194	Leverandøren skal sikre, at alle Leverandørens medarbejdere afleverer alle Informationsaktiver, som har været anvendt til Kontraktens opfyldelse, og som er i deres besiddelse, når deres ansættelse eller aftale ophører.	
Sikkerhedsbrud		
KTRL-157	Leverandøren skal i relation til Kontraktens opfyldelse sikre, at der foreligger skriftlige procedurer for håndtering af sikkerhedsbrud. Procedurerne skal omfatte håndtering af hhv. sikkerhedsbrud med og uden persondata involveret.	
KTRL-160	Leverandøren skal i relation til Kontraktens opfyldelse sikre, at de interne procedurer for rapportering af sikkerhedsbrud i medfør af KTRL-157, tager højde for eksterne tidsfrister, herunder Datatilsynets krav om anmeldelse af brud på persondatasaikkerheden inden for 72 timer. Ved brud på persondatasikkerheden, som vedrører Kundens data, skal Leverandøren anvende den blanket, som er vedlagt databehandleraftale til Kontrakten.	Ved brud på persondatasikkerheden , som involverer Kundens data, skal Leverandøren orientere om alle nødvendige detaljer for at vurdere bruddets omfang inden for 24 timer, fra bruddet konstateres, medmindre andet fremgår af databehandleraftalen.
KTRL-271	Leverandøren skal fastlægge ledelsesansvar og procedurer for at sikre hurtig, effektiv og planmæssig håndtering af sikkerhedsbrud relateret til Kontraktens opfyldelse. Er der mellem parterne indgået en databehandleraftale, vil der være en forpligtelse til at rapportere de informationer, som fremgår af skabelon i databehandleraftalen, til Kunden.	Procedurerne skal være dokumenterede.
KTRL-272	Leverandøren skal sikre, at sikkerhedsbrud relateret til Kontraktens opfyldelse rapporteres internt ad passende ledelseskanaler inden for en tidsramme, således at Kunden kan orienteres i passende tid, jf. KTRL-160.	
KTRL-275	Leverandøren skal sikre, at sikkerhed i relation til Kontraktens opfyldelse altid håndteres i overensstemmelse med de dokumenterede procedurer og gældende aftale med Kunden.	
Testdata		
KTRL-299	Såfremt Leverandøren skal drifte et udviklings- og/eller testmiljø for Kunden (fx for et specifikt system), skal Leverandøren have en proces for at sikre, at data, som skal lagres i udviklings- og testmiljøer (testdata) er anonymiserede, inden de lagres deri. I helt særlige tilfælde, hvor det ikke er muligt at teste på anonymiserede data (testdata), må dette kun ske efter konkret aftale med Kunden.	Ved konkret aftale om brug af produktionsdata i test til en specifik opgave, skal data slettes straks efter opgaven er udført. Er der taget backup af et miljø med produktionsdata, skal disse også slettes.

Webbrowsere og e-mails		
KTRL-051	Leverandøren skal i relation til Kontraktens opfyldelse minimere angrebsfladen og mulighederne for, at angribere kan manipulere medarbejderes adfærd via interaktion med webbrowsere og e-mailsystemer.	