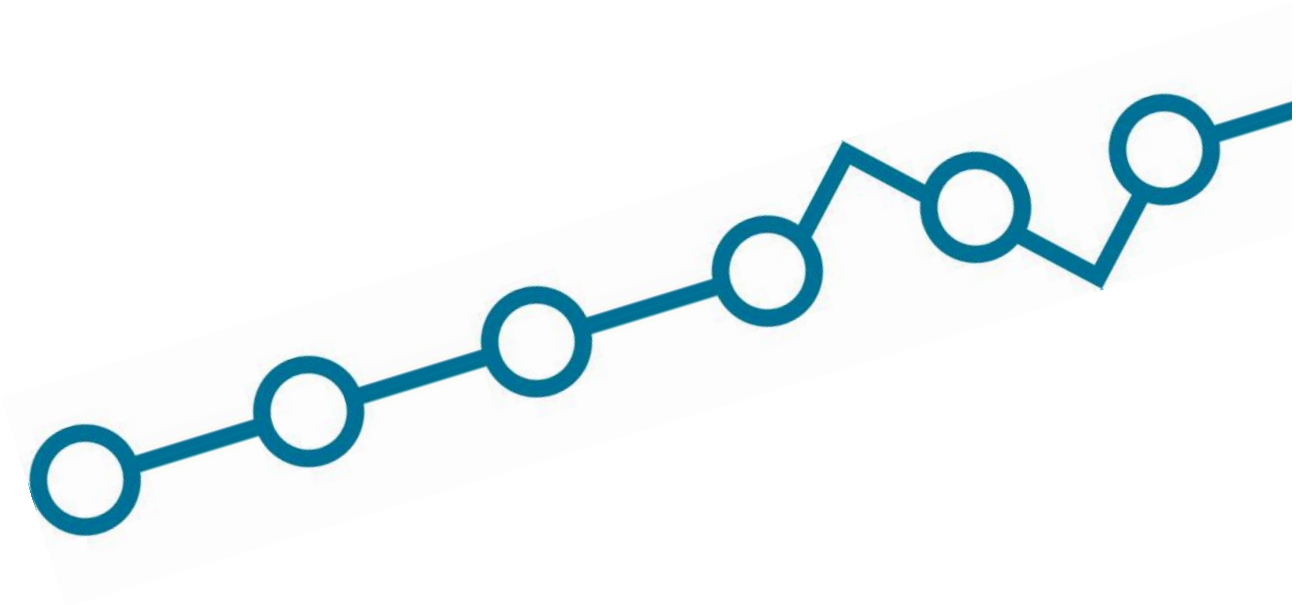
KOMBIT



KOMBIT sikkerhedspolitik

Indholdsfortegnelse

Indledning

Dette dokument indeholder KOMBITs politik for informationssikkerhed for leverandører, ”KOMBITs sikkerhedspolitik”.

Formålet med KOMBITs sikkerhedspolitik er at definere ansvaret for informationssikkerhed for de ydelser, som leverandører (”Leverandøren”) skal levere under en kontrakt med KOMBIT (”Kontrakten”)

Dette dokument opstiller krav til informationssikkerhed, som Leverandøren skal overholde for at sikre en passende beskyttelse af Anvendernes aktiver og Systemet, som Leverandøren forvalter og har adgang til i medfør af Kontrakten. Ved ”aktiver” forstås aktiver som begrebet anvendes i ISO 270001:2013.

Bilaget er opdelt i følgende:

- **Del 1**: Organisering, roller og ansvar
- **Del 2**: Politik for informationssikkerhed
- **Del 3**: Retningslinjer og kontrolmål til Leverandøren

Del 1: Organisering, roller og ansvar

På vegne af Anvenderne har KOMBIT udformet kravene til informationssikkerhed, som Leverandøren skal overholde i forbindelse med opfyldelse af Kontrakten.

De enkelte Anvendere, der benytter Systemet, er dataansvarlige for de personoplysninger, de lader behandle i Systemet, mens KOMBIT er databehandler for Anvenderne og dermed underlagt Anvendernes instruktionsbeføjelse, idet Anvenderne dog har givet KOMBIT fuldmagt til at overlade databehandlingsopgaven til en underdatabehandler, såfremt dette sker under samme betingelser, som der gælder i databehandleraftalen mellem KOMBIT og Anvenderne.

Som underdatabehandler til KOMBIT skal Leverandøren, på anmodning fra KOMBIT give KOMBIT eller dennes repræsentant tilstrækkelige oplysninger og kontroladgang til, at denne kan kontrollere Leverandørens overholdelse af indeværende dokuments krav til sikkerhed.

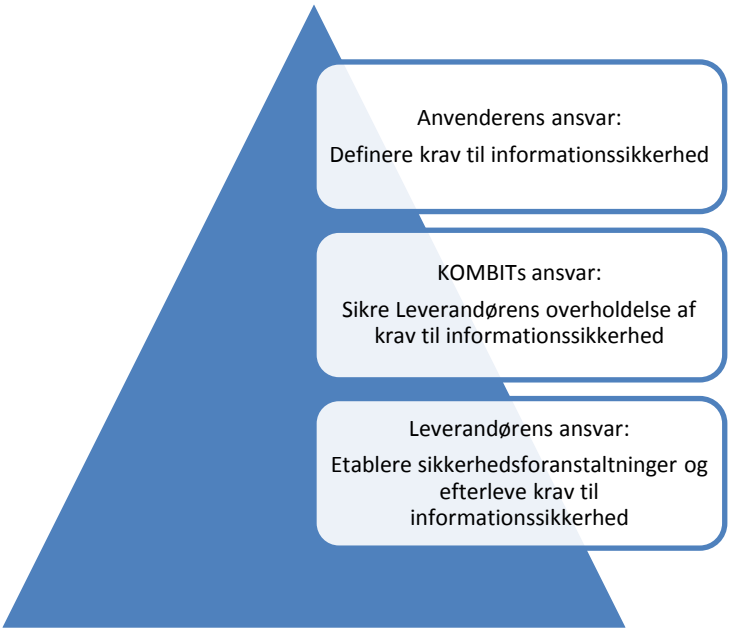
Derfor skal Leverandøren og KOMBIT i samarbejde sikre, at informationssikkerhedskravene i nærværende dokument bidrager til at minimere de risici, der er forbundet med Leverandørens behandling af Anvenderens aktiver og Systemet. Leverandøren skal mindst en gang årligt dokumentere, hvorledes kravene efterleves ved at få udarbejdet en revisionserklæring i henhold til ISAE 3402 type 2 sikkerhedsrevisionserklæring eller tilsvarende.

KOMBIT gennemfører regelmæssig opfølgning på, om Leverandøren opfylder kravene i nærværende dokument. Opfølgningen sker gennem ekstern auditering og målinger på effektiviteten af Leverandørens efterlevelse. Opfølgningen er baseret på de retningslinjer og kontrolmål, der er beskrevet i Del 3 i nærværende dokument.

Hvis Leverandøren benytter Underleverandører i forbindelse med opfyldelse af Kontrakten, er Leverandøren ansvarlig for at sikre, at Underleverandøren overholder kravene i nærværende dokument.

Hvis Leverandøren og/eller Underleverandører ikke efterlever kravene i nærværende dokument vil det blive anset som misligholdelse af Kontrakten. Misligholdelsen vil blive behandlet som anført i Del 3.

Nedenstående figur viser ansvarsfordelingen mellem Anvenderne, KOMBIT og Leverandøren.



Del 2: Politik for informationssikkerhed

Denne del af dokument indeholder KOMBITs krav til informationssikkerhed i forbindelse med Leverandørens opfyldelse af Kontrakten.

KOMBITs sikkerhedspolitik indeholder krav om, at Leverandøren skal efterleve ISO 27001:2013 eller tilsvarende samt relevant lovgivning, jf. punkt 18 i dette dokument.

For så vidt angår efterlevelse af ISO 270001:2013 eller tilsvarende gælder følgende ISO områder for Kontraktens tre modeller for så vidt angår drift og vedligeholdelse:

- Model 1: Totalleverandør
- Model 2: Applikationsdriftsleverandør og vedligeholdelsesleverandør
- Model 3: Applikationsvedligeholdelsesleverandør

	Model		
ISO område	1	2	3
5. INFORMATIONSSIKKERHEDSPOLITIKKER	X	X	X
6. ORGANISERING AF INFORMATIONSSIKKERHED	X	X	X
7. PERSONALESIKKERHED	X	X	X
8. STYRING AF AKTIVER	X	X	X
9. ADGANGSSTYRING	X	X	
10. KRYPTOGRAFI	X	X	
11. FYSISK SIKRING OG MILJØSIKRING	X		
12. DRIFTSSIKKERHED	X	X	
13. KOMMUNIKATIONSSIKKERHED	X	X	
14. ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF SYSTEMET	X	X	X
15. LEVERANDØRFORHOLD	X	X	X
16. STYRING AF INFORMATIONSSIKKERHEDSBRUD	X	X	
17. INFORMATIONSSIKKERHEDSASPEKTER VED NØD-, BEREDSKABS- OG REETABLERINGSSTYRING	X		
18. OVERENSSTEMMELSE	X	X	X

Opfølgningen på, om kravene overholdes, sker i henhold til de retningslinjer og kontrolmål, der er beskrevet for hvert ISO område i Del 3 i nærværende dokument.

Del 3: Retningslinjer og kontrolmål til Leverandøren

Kontrolmål anvendes til at kontrollere og sikre, at Leverandøren efterlever KOMBITs sikkerhedspolitik.

ISO-standardens 4 indledende kapitler beskriver standardens struktur og mål for Leverandørens styring af informationssikkerhed. Kapitel 5 og frem i ISO-standarden indeholder retningslinjerne og kontrolmål. For at sikre ensartethed mellem nærværende dokument og ISO-standarden er nedenstående retningslinjer og tilhørende kontrolmål nummereret i henhold til ISO-standarden.

Der er ikke specificeret kontrolmål til alle retningslinjer i ISO 27001:2013 standarden, da nogle af disse behandles i Kontrakten.

Kontrolmålene indeholder:

- **Formål**: Beskriver, hvorfor kontrolmålet er etableret, og sikrer at det afspejler den overordnede retningslinje for ISO-afsnittet.
- **Målepunkt**: Beskriver, hvordan kontrolmålet skal vurderes. Leverandøren skal sikre, at der etableres et tilfredsstillende datagrundlag, således at målingen kan gennemføres inden for det tidsinterval, der er beskrevet, hvilket sikrer, at målet er specifikt og målbart.
- **Tærskel**: Viser, hvad der kræves for, at Leverandøren overholder det givne kontrolmål.

Konsekvens for manglende overholdelse af Kontrolmål udgør misligholdelse af Kontrakten. Hvis manglende overholdelse udgør en sikkerhedsmæssig risiko i henhold til Kontrakten, behandles dette i overensstemmelse med Kontrakten.

5. Informationssikkerhedspolitikker

Formål

Leverandøren er bekendt med KOMBITs sikkerhedspolitik og retningslinjer, som er udarbejdet på vegne af Anvenderne.

Leverandøren har udarbejdet en politik for informationssikkerhed, der inkluderer kravene i nærværende dokument. Leverandørens politik for informationssikkerhed indeholder en overordnet politik for informationssikkerhed og underliggende retningslinjer for hvert ISO område.

Informationssikkerhedspolitikken er godkendt af Leverandørens ledelse og offentliggjort hos Leverandøren, herunder kommunikeret til alle ansatte og relevante samarbejdspartnere. Informationssikkerhedspolitikken revurderes med jævne mellemrum (minimum én gang årligt) eller ved omfattende ændringer i organisationen, som har indflydelse på informationssikkerheden, for at sikre, at informationssikkerhedspolitikken er passende, tilstrækkelig og effektiv.

Retningslinjer

Leverandøren sikrer, at informationssikkerhedspolitikken er godkendt af Leverandørens ledelse og gjort offentligt tilgængelig i dennes organisationen samt kommunikeret til alle ansatte og relevante samarbejdspartnere. Informationssikkerhedspolitikken angiver de retningslinjer, som Leverandørens ledelse har besluttet med henblik på nærmere at fastlægge et tilstrækkeligt sikkerhedsniveau til overholdelse af kravene i nærvæ-

rende dokument, således at dette niveau opretholdes. Herudover beskrives ansvar og roller i forhold til informationssikkerheden og styringen af hændelser, der kan have indflydelse på informationssikkerheden i forbindelse med Leverandørens opfyldelse af Kontrakten.

Leverandøren er ansvarlig for at sikre, at det er muligt at følge op på efterlevelse af de enkelte sikkerhedskrav.

Kontrolmål

5.1.1 Politikker for informationssikkerhed

Leverandørens ledelse skal fastlægge og godkende en informationssikkerhedspolitik, som skal offentliggøres og kommunikeres til medarbejdere og relevante samarbejdspartnere. Informationssikkerhedspolitikken skal opbygges i henhold til ISO 27001:2013 eller tilsvarende, opfylde relevant lovgivning, jf. punkt 18 i dette dokument, samt efterleve kravene i nærværende dokument.

Politikker for informationssikkerhed		
KPI-5.1.1	**Formål:**	Leverandørens ledelse skal fastlægge og godkende en informationssikkerhedspolitik, som skal offentliggøres og kommunikeres til medarbejdere og relevante samarbejdspartnere. Politikken skal opbygges i henhold til ISO 27001:2013 eller tilsvarende, opfylde relevant lovgivning, jf. punkt 18 i dette dokument, samt efterleve kravene i indeværende dokument.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Politikken skal være dokumenteret og skal opdateret mindst én gang årligt. Tærsklen overskrides, når politikken ikke er dokumenteret og/eller ikke har været opdateret i 365 dage siden sidste opdatering. Tærsklen overholdes efter overskridelse, når politikken er dokumenteret og/eller opdateret.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandøren har ikke en politik for informationssikkerhed
1	**Ad hoc / intuitiv**	Leverandøren har en politik for informationssikkerhed, men denne er ikke standardiseret og procedurer udarbejdes ad hoc af individuelle afdelinger.
2	**Defineret**	Politikken er standardiseret, dokumenteret og kommunikeret. Medarbejderne følger gældende sikkerhedskrav.
3	**Styret og målbar**	Politikken er standardiseret, dokumenteret og kommunikeret. Medarbejderne følger gældende sikkerhedskrav. Politikken vurderes løbende og gældende kontroller justeres.
4	**Optimeret**	Politikken er standardiseret, dokumenteret og kommunikeret. Medarbejderne følger gældende sikkerhedskrav. Politikken vurderes løbende og sammenholdes med den overordnede strategi og gældende kontroller justeres og optimeres.

6. Organisering af informationssikkerhed

Formål

Leverandøren skal sikre et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og vedligeholdelsen af informationssikkerhed i organisationen. Herunder varetagelse af ansvarsplacering, udmønte de generelle retningslinjer i specifikke forretningsgange og instrukser samt sikre løbende opfølgning på implementering og efterlevelse af informationssikkerhedspolitikken, opfylde relevant lovgivning, jf. punkt 18 i dette dokument, samt efterleve kravene i indeværende dokument.

Retningslinjer

Leverandøren skal etablere en intern organisering, der sikrer, at kravene i nærværende dokument overholdes. Det overordnede ansvar for informationssikkerhed er etableret af Leverandøren, og Leverandørens ledelse har ansvaret for at implementere informationssikkerhed i organisationen, sikre relevante kontroller er til stede, og at disse er effektive.

Kontrolmål

6.1.1 Roller og ansvarsområder for informationssikkerhed
Alle ansvarsområder for informationssikkerhed (jf. ISO 27001:2013 eller tilsvarende) skal defineres og fordeles. Leverandøren skal sikre, at ansvaret for alle informationssikkerhedsaktiviteter, herunder beskyttelse af Anvendernes aktiver og udførelsen af særlige sikkerhedsprocedurer er klart defineret, herunder at ansvaret er placeret og fremgår af funktionsbeskrivelser.

6.1.2 Funktionsadskillelse

Funktionsadskillelse		
KPI-6.1.2	**Formål:**	Modstridende funktioner og ansvarsområder hos Leverandøren skal adskilles for at begrænse muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af Anvendernes aktiver.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Over 2 personer/systemer, pr år, der ikke opfylder kravet om funktionsadskillelse. Såfremt en audit påviser, at mere end 2 personer/ systemer ikke er funktionsadskilt er tærsklen overskredet, indtil forholdet er bragt i orden.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er ikke etableret funktionsadskillelse
1	**Ad hoc / intuitiv**	Adskillelse af udviklingsmiljøet og Driftsmiljøet. Man har tænkt på funktionsadskillelse, men der er ikke en fuldstændig konsekvent procedure for at opretholde det.

2	**Defineret**	Adskillelse af udviklingsmiljøet og Driftsmiljøet. Der findes en procedure for tildeling af ansvarsområder og der er en opdateret oversigt over, hvilke brugere som er tildelt hvilke ansvarsområder.
3	**Styret og målbar**	Adskillelse af udviklingsmiljøet og Driftsmiljøet. Der findes en procedure for tildeling af ansvarsområder og der er en opdateret oversigt over hvilke brugere, som er tildelt hvilke ansvarsområder. Der foretages løbende opfølgning på henholdsvis brugere med adgang til udviklingsmiljø og Driftsmiljøet.
4	**Optimeret**	Adskillelse af udviklingsmiljøet og Driftsmiljøet. Der findes en procedure for tildeling af ansvarsområder og der er en opdateret oversigt over hvilke brugere, som er tildelt hvilke ansvarsområder. Der foretages løbende automatiseret kontrol af henholdsvis brugere med adgang til udviklingsmiljø og Driftsmiljøet. Funktionsadskillelse er fuldt systemunderstøttet.

6.1.5 Informationssikkerhed ved projektstyring

Informationssikkerhed ved projektstyring		
KPI-6.1.5	**Formål:**	Leverandøren skal sikre, at informationssikkerhed, herunder hensyn til beskyttelse af fortrolighed, integritet og tilgængelighed varetages ved projektstyring, uanset projekttype, både under udvikling, vedligehold og videreudvikling.
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	1 projekt, der ikke opfylder informationssikkerhed ved projektstyring. Tærsklen er overskredet fra det tidspunkt Leverandøren konstaterer eller burde have konstateret, at et igangværende projekt ikke overholder Informationssikkerhed, og indtil projektet overholder informationssikkerhed.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er ikke identificeret et særligt behov for at styre informationssikkerhedsrisici i forhold til projekter.
1	**Ad hoc / intuitiv**	Der anvendes en række metoder og tilgange i organisationen på tværs af projekter. Sikkerhed og risici bliver delvist adresseret. Sikkerhedskontroller tilføres ofte efter lancering til produktionsmiljøet.
2	**Defineret**	Der anvendes en ensartet metodik og tilgang for større projekter, hvori sikkerhed og risici adresseres. Ensartede sikkerhedsarkitekturprincipper overvejes.
3	**Styret og målbar**	Projekter stoppes, hvis sikkerhedskrav ikke bliver mødt. Der findes specialiserede metodikker for at styre sikkerhedskrav ift. behovet og risikoen i

		det enkelte projekt, herunder adressering af lovmæssige krav. Sikkerheds-arkitektur-komponenter er integreret i udviklingen.
4	**Optimeret**	Sikkerhed og risikostyring er en integreret del af projekter og udvikling, inklusiv arkitekturprincipper. Arkitekturprincipper justeres i henhold til ændringer i lovgivning, kontraktlige krav og øvrige regulativer. Der er løbende vurdering af gældende principper for at sikre bedst mulige designs og fremtidige løsninger

7. Personalesikkerhed

Formål

Minimering af risici forbundet med Leverandørens og eventuelle Underleverandørers medarbejdere, ved at alle relevante medarbejdere på forhånd er bevidste om og efterlever deres ansvar i forbindelse med arbejde med Systemet og data, som behandles i medfør af Kontrakten. Medarbejdergrupper hos Leverandøren eller Underleverandører, der kan udgøre en større risiko, skal identificeres på forhånd.

Sikre, at alle relevante medarbejdere er opmærksomme på relevante trusler og har den fornødne viden til at opretholde det sikkerhedsniveau, som kræves på baggrund af de stillede krav. Leverandørens ledelse har ansvar for, at medarbejdere kan opretholde dette niveau.

Sikring af, at ophørte medarbejdere forlader Leverandøren med mindst mulig risiko for Systemet og de data, som behandles i medfør af Kontrakten.

Retningslinjer

Leverandøren skal sikre, at alle relevante medarbejdere har den fornødne viden om deres ansættelsesforhold, så medarbejderne kan opretholde deres ansvar for sikkerheden i forbindelse med opfyldelse af Kontrakten. Dette omfatter både fastansatte såvel som midlertidigt ansatte.

Ved ansættelse af medarbejdere, der skal arbejde med Systemet og data relateret til Systemet, skal disse gennemgå en screeningsproces for at undgå uhensigtsmæssige ansættelser. Dette gælder både faste og midlertidige ansættelser.

Ved enhver ansættelse af medarbejdere, der skal bistå Leverandøren med opfyldelse af Kontrakten, skal den ansatte og Leverandøren underskrive en kontrakt om betingelserne for ansættelsen. Betingelserne skal indeholde de ansættelsesvilkår og –betingelser som fremgår af KPI-7.1.2.

Ved endt ansættelse skal en fastlagt procedure sikre, at medarbejderen er oplyst om sine fortsatte forpligtelser. Dette indebærer bl.a. en pligt for Leverandøren til at sikre, at tavshedspligten ikke ophører ved ansættelsens ophør.

Kontrolmål

7.1.2 Ansættelsesvilkår og -betingelser

Ansættelsesvilkår og -betingelser		
KPI-7.1.2.	**Formål:**	Leverandøren skal sikre, at samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, er underlagt følgende betingelser: • Tavshedserklæring, såfremt medarbejderen skal udføre arbejde med adgang til Systemet. • Medarbejderens retslige ansvar, herunder virksomhedens ophavsret og eventuel datalovgivning, jf. punkt 18 i dette dokument • Medarbejderens ansvar i forbindelse med behandling af informationer • Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen og håndhæves
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Betingelser er beskrevet og kommunikeret skriftligt til den enkelte medarbejder og de er accepteret af medarbejderen.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Krav til medarbejderen i forhold til informationssikkerhed adresseres ikke.
1	**Ad hoc / intuitiv**	Der er hos Leverandøren en bevidsthed om, at nævnte betingelser er vigtige, men der er ikke en dokumenteret formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med disse.
2	**Defineret**	Der er en formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med nævnte betingelser. Dette attesteres skriftligt af medarbejderen ved indgåelse af samarbejde.
3	**Styret og målbar**	Der er en formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med nævnte betingelser. Dette attesteres skriftligt af medarbejderen ved indgåelse af samarbejde og revideres regelmæssigt.
4	**Optimeret**	Der er en formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med nævnte betingelser. Dette attesteres skriftligt af medarbejderen ved indgåelse af samarbejde og revideres regelmæssigt. Procedurerne er systemunderstøttet, og der foretages løbende målinger på deres effektivitet.

7.2.1 Ledelsesansvar

Ledelsesansvar		
KPI-7.2.1.	**Formål:**	Leverandørens ledelse skal sikre, at alle relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, opretholder informationssikkerhed i overensstemmelse med kravene i nærværende dokument.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Procedurer er beskrevet og overholdt.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er hos Leverandøren ikke en ledelsesstyret tilgang til, at samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, skal opretholde informationssikkerhed.
1	**Ad hoc / intuitiv**	Der er hos Leverandøren en bevidsthed i ledelsen om, at samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, skal opretholde informationssikkerhed i overensstemmelse med kravene i nærværende dokument, men der er ikke en dokumenteret formel procedure for at sikre dette.
2	**Defineret**	Der er en ledelsesforankret formel procedure for, at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med deres forpligtelser for at opretholde informationssikkerhed i overensstemmelse med kravene.
3	**Styret og målbar**	Der er en ledelsesforankret formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med deres forpligtelser for at opretholde informationssikkerhed i overensstemmelse med kravene i nærværende dokument. Den enkelte medarbejder attesterer skriftligt disse forpligtelser årligt.
4	**Optimeret**	Der er en ledelsesforankret formel procedure for at gøre samtlige relevante medarbejdere, herunder medarbejdere hos eventuelle Underleverandører, bekendte med deres forpligtelser for at opretholde informationssikkerhed i overensstemmelse med kravene i nærværende dokument. Den enkelte medarbejder attesterer skriftligt disse forpligtelser årligt, og der udføres regelmæssig awareness aktiviteter for at sikre forankringen hos den enkelte.

8. Styring af aktiver

Formål

Beskyttelse af Anvenderens aktiver og Systemet, herunder fysiske, data og informationsmæssige aktiver, gennem identifikation, angivelse af ejer samt beskrivelse af korrekt brug.

Sikring af information og Systemet på et passende niveau, som står i forhold til informationens klassifikation og betydning for Anvender.

Retningslinjer

Alle Anvenderes aktiver skal identificeres, og det enkelte aktiv skal tildeles en ansvarlig hos Leverandøren.

Kontrolmål

8.1.1 Fortegnelse over aktiver

Fortegnelse over aktiver		
KPI-8.1.1.	**Formål:**	Alle aktiver, der er omfattet af Kontrakten, skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over aktiverne.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Aktivfortegnelsen er dokumenteret og vedligeholdt. Tærsklen er overskredet, når alle aktiver ikke er angivet i fortegnelsen

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der findes ingen formaliseret styring af aktiver.
1	**Ad hoc / intuitiv**	Leverandøren har identificeret, at styring af aktiver bør adresseres. Der findes få standardiserede processer, som tager hånd om styring af aktiver.
2	**Defineret**	Aktivfortegnelsen er dokumenteret og indeholder relevante beskrivelser af delkomponenter, fysisk og logisk placering, ejerskab, m.v.
3	**Styret og målbar**	Aktivfortegnelsen er dokumenteret og indeholder relevante beskrivelser af delkomponenter, fysisk og logisk placering, ejerskab, m.v. Alle fortegnelser bliver løbende opdateret på baggrund af reelle data om de enkelte aktiver.
4	**Optimeret**	Aktivfortegnelsen er dokumenteret og indeholder relevante beskrivelser af delkomponenter, fysisk og logisk placering, ejerskab, m.v. Alle fortegnelser bliver løbende opdateret på baggrund af reelle data om de enkelte aktiver. Opdatering foretages automatisk.

9. Adgangsstyring

Formål

Leverandøren skal have retningslinjer for adgangsstyring, og disse skal dokumenteres og evalueres på grundlag af forretnings- og sikkerhedsmæssige krav til adgang.

Leverandøren skal sikre, at kun autoriserede brugere har adgang til Systemet eller Driftsmiljøet, samt at uautoriserede brugere forhindres adgang, for derved at undgå kompromittering eller tyveri.

Retningslinjer

Adgange til Systemet og Driftsmiljøet tildeles altid med udgangspunkt i "need-to-know"/ "need-to-have" og "least privilege"-principperne, så det tilsikres, at adgange er tildelt brugere med et arbejdsbetinget behov, uanset hvilken form for it-udstyr der anvendes.

Der tages altid hensyn til relevant lovgivning, jf. punkt 18 i dette dokument og kontraktlige forpligtigelser som en del af adgangsstyringen til Systemet.

Leverandøren skal sikre imod akkumulering af rettigheder for individuelle brugere, og der er implementeret funktionsadskillelse som en del af adgangsstyringen, således at der findes funktionsadskillelse.

Kontrolmål

9.1.2 Politik for adgangsstyring

Politik for adgangsstyring		
KPI-9.1.2.	**Formål:**	Leverandøren skal fastlægge en politik for adgangsstyring og håndhæve denne. Politikken og dertilhørende retningslinjer skal dokumenteres og gennemgås på baggrund af forretnings- og informationssikkerhedskrav.
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	Politikken skal følge ISO27001:2013 standarden eller tilsvarende. Tærsklen er overskredet, når Leverandørens politik ikke følger ISO27001:2013 standarden eller tilsvarende.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der findes ikke en politik for adgangsstyring
1	**Ad hoc / intuitiv**	Adgangsstyring foretages ad hoc og er ikke ensartet på tværs af Systemet. Det er op til individuelle systemansvarlige at styre adgange på Systemet.
2	**Defineret**	Der findes en standardiseret politik for adgangsstyring på tværs af Systemet. Systemansvarlige er bekendt hermed og følger politikken.

3	**Styret og målbar**	Politikken for adgangsstyring på tværs af Systemet vurderes jævnligt, og der er etableret foranstaltninger, som sikrer, at systemmæssige afvigelser fra politikken rapporteres og vurderes jævnligt.
4	**Optimeret**	Politikken for adgangsstyring på tværs af Systemet vurderes jævnligt, og der er etableret foranstaltninger, som sikrer, at systemmæssige afvigelser fra politikken rapporteres og vurderes jævnligt. Politikken sikrer, at afvigelser vurderes og kontroller løbende justeres herefter.

9.2.3 Styring af privilegerede adgangsrettigheder

Styring af privilegerede adgangsrettigheder		
KPI-9.2.3	**Formål:**	Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres for Leverandørens medarbejdere. Ved privilegerede adgangsrettigheder forstås muligheden for at omgå system- eller applikationskontroller. Det er Leverandørens ansvar at administrere privilegerede adgangsrettigheder, herunder at formalisere anvendelsen af privilegerede adgangsrettigheder. Tildelingen af privilegerede adgangsrettigheder sker, så det er muligt at skelne mellem brugerkonti med privilegerede adgangsrettigheder og almindelige brugerkonti. Der er etableret en procedure, som sikrer, at der kun kan opnås privilegerede adgangsrettigheder i nødstilfælde (nødbrugere) med tilhørende revisionsspor for anvendelsen.
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	Tildeling af privilegerede rettigheder er veldokumenteret og opdateret. Tærsklen er overskrevet, såfremt privilegerede rettigheder ikke er veldokumenteret og opdateret, og indtil de er bragt til en tilstand, hvor de er veldokumenteret og opdateret.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er ingen kontrol med brugere med privilegerede adgangsrettigheder.
1	**Ad hoc / intuitiv**	Der er ikke etableret en procedure for styring af privilegerede adgangsrettigheder. Tildeling af privilegerede adgangsrettigheder foretages ad hoc.
2	**Defineret**	Der er etableret en procedure for styring af privilegerede adgangsrettigheder. Proceduren er kendt af de ansvarlige medarbejdere hos Leverandøren, og tildelingen af privilegerede adgangsrettigheder følger proceduren og dokumenteres.

3	**Styret og målbar**	Der er etableret en procedure for styring af privilegerede adgangsrettigheder. Proceduren er kendt af de ansvarlige medarbejdere hos Leverandøren, og tildelingen af privilegerede adgangsrettigheder følger proceduren og dokumenteres. Der udføres regelmæssig revision af brugere med privilegerede adgangsrettigheder.
4	**Optimeret**	Der er etableret en procedure for styring af privilegerede adgangsrettigheder. Proceduren er kendt af de ansvarlige medarbejdere hos Leverandøren, og tildelingen af privilegerede adgangsrettigheder følger proceduren og dokumenteres. Der udføres regelmæssig revision af brugere med privilegerede adgangsrettigheder. Der foretages løbende rapportering og målinger for antallet af brugere med privilegerede adgangsrettigheder.

9.2.5 Gennemgang af brugeradgangsrettigheder

Gennemgang af brugeradgangsrettigheder		
KPI-9.2.5.	**Formål:**	Leverandøren skal med jævne mellemrum gennemgå brugernes adgangsrettigheder. Der skal af Leverandøren foretages stikprøvevis opfølgning på tildelingen af privilegerede adgangsrettigheder. Der opbevares dokumentation for udførte opfølgninger.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Dokumentation for gennemgang skal være opdateret. Tærsklen er overskredet, såfremt Leverandøren konstaterer eller burde have konstateret, at dokumentation for gennemgang ikke er opdateret, og indtil dokumentation for gennemgang er opdateret

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er ikke etableret en procedure for gennemgang af brugernes adgangsrettigheder.
1	**Ad hoc / intuitiv**	Leverandøren foretager stikprøvevis opfølgning på tildelingen privilegerede adgangsrettigheder, men dette følger ikke en formel procedure.
2	**Defineret**	Leverandøren har en formel procedure for at gennemgå brugernes adgangsrettigheder. Leverandøren foretager stikprøvevis opfølgning på tildelingen af privilegerede adgangsrettigheder. Der opbevares dokumentation for udførte opfølgninger.
3	**Styret og målbar**	Leverandøren har en formel procedure for gennemgang af brugernes adgangsrettigheder. Der foretages et komplet udtræk af tildelte brugerrettigheder på Systemet, og disse gennemgås og godkendes af systemansvarlig hos Leverandør. Der opbevares dokumentation for udførte opfølg-

		ninger, og disse sammenholdes over tid.
4	**Optimeret**	Leverandøren har en formel procedure for gennemgang af brugernes adgangsrettigheder. Der foretages et komplet udtræk af tildelte brugerrettigheder på Systemet, og disse gennemgås og godkendes af systemansvarlig hos Leverandør. Der opbevares dokumentation for udførte opfølgninger, og disse sammenholdes over tid. Hele proceduren er systemunderstøttet.

10. Kryptografi

Formål

Formålet med disse krav er at sikre korrekt og effektiv brug af kryptografi for at beskytte datas fortrolighed, autenticitet og/eller integritet.

Retningslinjer

Behovet for kryptering skal identificeres ud fra en vurdering af, hvor metoden som sikringsforanstaltning kan imødegå behovet for sikring af datas fortrolighed, autenticitet og/eller integritet. Ved anvendelse af kryptering skal der desuden tages højde for nøglehåndtering.

Kontrolmål

10.1.1 Politik for anvendelse af kryptografi

Politik for anvendelse af kryptografi		
KPI-10.1.1.	**Formål:**	Leverandøren skal have en politik for anvendelse af kryptografi til beskyttelse af Anvendernes data i Systemet, og håndhæve denne. Der skal være udarbejdet konkrete retningslinjer for brugen af kryptografi, som overholder kravet til "stærk kryptering" jf. *Bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning* Data og underliggende infrastruktur skal beskyttes ved transmission af fortrolige oplysninger.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Politikken er dokumenteret og vedligeholdt. Tærsklen er overskrevet, såfremt politikken ikke er dokumenteret og vedligeholdt, og indtil politikken er dokumenteret og vedligeholdt.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandøren har ikke defineret en politik eller retningslinjer for anvendelse af kryptografi.

1	**Ad hoc / intuitiv**	Der findes ikke en politik for anvendelse af kryptografi, men der kan være retningslinjer for Systemet
2	**Defineret**	Der findes en politik for anvendelse af kryptografi, og medarbejderne er bekendt med denne. Politikken tilsikrer ligeledes beskrivelse af retningslinjer for håndtering af nøgler. Medarbejderne er bekendt med politikken, men der kan findes afvigelser fra denne.
3	**Styret og målbar**	Politikken for anvendelse af kryptografi er defineret, og der er opsat krav i f.eks. projekter til, hvordan kryptografi skal anvendes, samt de foranstaltninger som tages i forbindelse hermed. Der foretages jævnlige målinger på anvendt kryptografi på tværs af projekter.
4	**Optimeret**	Politikken for anvendelse af kryptografi er defineret, og der er opsat krav i f.eks. projekter til, hvordan kryptografi skal anvendes, samt de foranstaltninger som tages i forbindelse hermed. Der foretages jævnlige målinger på anvendt kryptografi på tværs af projekter. Politikken og tilhørende retningslinjer justeres løbende i forhold til god praksis.

10.1.2 Administration af nøgler

Administration af nøgler		
KPI-10.1.2.	**Formål:**	Leverandøren skal udarbejde, implementere og håndhæve en politik for anvendelse og beskyttelse af, samt levetid for, krypteringsnøgler gennem hele deres livscyklus. Nøglehåndteringen skal understøtte procedurerne for generering, distribution, lagring, ændring, opdatering, tilbagekaldelse, aktivering, genskabelse og destruktion af nøgler og offentlige nøglecertifikater. Aktiviteter i forbindelse med nøglehåndtering skal logges.
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Politikken er dokumenteret og vedligeholdt. Tærsklen er overskredet, når politikken ikke er dokumenteret og vedligeholdt, og indtil politikken er dokumenteret og vedligeholdt.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandøren har ikke defineret en politik eller retningslinjer for administration af nøgler
1	**Ad hoc / intuitiv**	Der findes ikke en politik for administration af nøgler, men der kan være retningslinjer for Systemet.
2	**Defineret**	Der findes en politik for administration af nøgler, som beskriver håndtering

		af nøgler, herunder generering, distribution, lagring, ændring, opdatering, tilbagekaldelse, aktivering, genskabelse og destruktion af nøgler og offentlige nøglecertifikater. Medarbejderne er bekendt med politikken, og den vedligeholdes løbende.
3	**Styret og målbar**	Der findes en politik for administration af nøgler, som beskriver håndtering af nøgler, herunder generering, distribution, lagring, ændring, opdatering, tilbagekaldelse, aktivering, genskabelse og destruktion af nøgler og offentlige nøglecertifikater. Medarbejderne er bekendt med politikken, og den vedligeholdes løbende. Al administration af nøgler foretages i overensstemmelse med politikken.
4	**Optimeret**	Der findes en politik for administration af nøgler, som beskriver håndtering af nøgler, herunder generering, distribution, lagring, ændring, opdatering, tilbagekaldelse, aktivering, genskabelse og destruktion af nøgler og offentlige nøglecertifikater. Medarbejderne er bekendt med politikken, og den vedligeholdes løbende. Al administration af nøgler foretages i overensstemmelse med politikken. Politikken og tilhørende retningslinjer justeres løbende i forhold til god praksis og er systemunderstøttet.

11. Fysisk sikring og miljøsikring

Håndteres i Kontrakten.

12. Driftssikkerhed

Håndteres i Kontrakten.

13. Kommunikationssikkerhed

Håndteres i Kontrakten.

14. Anskaffelse, udvikling og vedligeholdelse af Systemet

Håndteres i Kontrakten.

15. Leverandørforhold

Om betydningen af anvendelse af eventuelle Underleverandører henvises til Del 1. Krav i dette afsnit skal efterleves af Leverandøren, hvis denne anvender Underleverandører til at levere ydelser i forbindelse med opfyldelse af Kontrakten.

Formål

Leverandøren er ansvarlig for alle sine Underleverandører. Det vil sige, at Leverandøren sikrer, at sine Underleverandører opfylder samme betingelser, som Leverandøren selv, herunder beskyttelse af Anvendernes aktiver og Systemet, såfremt Underleverandører har adgang hertil.

Retningslinjer

Leverandøren sikrer, at alle nedenstående kontrolmål er opfyldt, inden Underleverandører får adgang til Anvendernes aktiver og Systemet. Tilsvarende gælder, hvis Underleverandører får adgang til Leverandørens infrastruktur, som kan påvirke informationssikkerheden af Anvendernes aktiver og Systemet.

Kontrolmål

15.1.1 Informationssikkerhedspolitik for leverandørforhold

Informationssikkerhedspolitik for leverandørforhold		
KPI-15.1.1	**Formål:**	At minimere de risici, der er forbundet med Underleverandørs adgang til Anvendernes aktiver, Systemet og Leverandørens infrastruktur skal aftales og dokumenteres. Leverandøren skal udarbejde en risikovurdering af samarbejdet mellem Leverandøren og Underleverandøren, inden samarbejdet indgås, og den tilbageværende risiko skal behandles af Leverandøren. Leverandøren skal sikre, at Underleverandørens medarbejdere er bekendte med og overholder Leverandørens politik for informationssikkerhed og dermed kravene i nærværende dokument.
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	Leverandørens politik for informationssikkerhed og kravene i nærværende dokument overholdes af Underleverandøren.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandørens kontrakter med Underleverandører beskriver ikke krav til sikkerhed.
1	**Ad hoc / intuitiv**	Leverandørens kontrakter med Underleverandører beskriver krav til sikkerhed, men der er ikke entydig reference til Leverandørens politik

		for informationssikkerhed og kravene i nærværende dokument
2	**Defineret**	Leverandørens kontrakter med Underleverandører beskriver entydigt Leverandørens politik for informationssikkerhed og kravene i nærværende dokument, der håndhæves
3	**Styret og målbar**	Leverandørens kontrakter med Underleverandører beskriver entydigt Leverandørens politik for informationssikkerhed og kravene i nærværende dokument. Yderligere sikkerhedstiltag er baseret på risikovurdering og er aftalt og implementeret. Der foretages regelmæssig evaluering af Underleverandører og mangler udbedres.
4	**Optimeret**	Leverandørens kontrakter med Underleverandører beskriver entydigt Leverandørens politik for informationssikkerhed og kravene i nærværende dokument og samtlige Underleverandører sikrer overholdelse af disse regelmæssigt. Yderligere sikkerhedstiltag er baseret på risikovurdering og er aftalt og implementeret.

16. Styring af informationssikkerhedsbrud

Formål

Leverandøren skal sikre korrekt og sikker styring af informationssikkerhedshændelser og -brud.

Leverandøren skal sikre, at Leverandørens medarbejdere og eventuelle Underleverandører er bekendt med Kontraktens krav om rapportering af hændelser og sårbarheder, der kan have indflydelse på Anvendernes aktiver og Systemet.

Ansvar og procedurer er på plads til effektivt at håndtere sikkerhedshændelser og sårbarheder effektivt, når de opstår. Der er etableret procedurer for løbende forbedringer af reaktioner på, overvågning og vurdering af sikkerhedsbrud relateret til Leverandørens opfyldelse af Kontrakten.

Retningslinjer

Leverandøren sikrer, at Leverandørens medarbejdere og eventuelle Underleverandører er bekendt med Kontraktens krav om rapportering af hændelser og sårbarheder, der kan have indflydelse på Anvendernes aktiver og Systemet. Svagheder i Systemet rapporteres på en måde, så Leverandøren kan rette op på og kompensere for sikkerhedsbrud.

Kontrolmål

16.1.1 Ansvar og procedure

Ansvar og procedure

KPI-16.1.1.	**Formål:**	Leverandøren har ansvaret for at sikre, at der er procedurer, som sikrer hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.
	Målepunkt:	4, jf. nedenfor.
	Tærskel:	Procedurer skal være dokumenteret, overholdt og vedligeholdt.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der er ikke defineret en procedure for håndtering af informationssikkerhedshændelser og –brud.
1	**Ad hoc / intuitiv**	Der er ikke defineret en procedure for håndtering af informationssikkerhedshændelser og –brud, men der findes retningslinjer på udvalgte områder.
2	**Defineret**	Der er defineret en procedure for håndtering af informationssikkerhedshændelser og –brud. Retningslinjerne følger proceduren, og informationshændelser og –brud dokumenteres.
3	**Styret og målbar**	Der er defineret en procedure for håndtering af informationssikkerhedshændelser og –brud. Retningslinjerne følger proceduren, og informationshændelser og –brud dokumenteres, følges op og rapporteres. Der måles på mængde og alvorlighed af hændelser.
4	**Optimeret**	Der er defineret en procedure for håndtering af informationssikkerhedshændelser og –brud. Retningslinjerne følger proceduren, og informationshændelser og –brud dokumenteres, følges op og rapporteres. Der måles på mængde og alvorlighed af hændelser. Proceduren og retningslinjer opdateres regelmæssigt på baggrund af erfaringer.

16.1.2 Rapportering af informationssikkerhedshændelser

Rapportering af informationssikkerhedshændelser		
KPI-16.1.2.	**Formål:**	Leverandøren skal rapportere informationssikkerhedshændelser til KOMBIT samt til evt. berørte interessenter.
	Målepunkt:	4, jf. nedenfor.
	Tærskel:	Samtlige informationssikkerhedshændelser, der er kritiske, alvorlige eller betydende skal rapporteres.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Informationssikkerhedshændelser rapporteres ikke.

1	**Ad hoc / intuitiv**	Der er ikke en formaliseret procedure for rapportering af informationssikkerhedshændelser, men dette sker ad hoc afhængig af den enkelte hændelse, og den medarbejdergruppe der er involveret.
2	**Defineret**	Der er en formaliseret procedure for rapportering af informationssikkerhedshændelser. Relevante medarbejdergrupper er bekendte med denne procedure og følger den.
3	**Styret og målbar**	Der er en formaliseret procedure for rapportering af informationssikkerhedshændelser. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Proceduren testes regelmæssigt og effektiviteten rapporteres.
4	**Optimeret**	Der er en formaliseret procedure for rapportering af informationssikkerhedshændelser. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Proceduren testes regelmæssigt og effektiviteten rapporteres. Proceduren justeres jævnligt på baggrund af erfaringer og resultat af udførte test.

16.1.3 Rapportering af informationssikkerhedssvagheder.

Rapportering af informationssikkerhedssvagheder		
KPI-16.1.3.	**Formål:**	Leverandøren har pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i Systemet
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	Samtlige informationssikkerhedssvagheder, der afdækkes, og som er kritiske, alvorlige eller betydende, skal rapporteres

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandøren har ikke en procedure for at rapportere informationssikkerhedssvagheder.
1	**Ad hoc / intuitiv**	Leverandøren har ikke en formaliseret procedure for at rapportere informationssikkerhedssvagheder, men informationssikkerhedssvagheder rapportere ad hoc.
2	**Defineret**	Leverandøren har en formaliseret procedure for at rapportere informationssikkerhedssvagheder. Relevante medarbejdergrupper er bekendte med denne procedure og følger den.
3	**Styret og målbar**	Leverandøren har en formaliseret procedure for rapportering af informationssikkerhedssvagheder. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Proceduren testes regelmæssigt og

		effektiviteten rapporteres.
4	**Optimeret**	Der er en formaliseret procedure for rapportering af informationssikkerhedssvagheder. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Proceduren testes regelmæssigt og effektiviteten rapporteres. Proceduren justeres jævnligt på baggrund af erfaringer og resultat af udførte test.

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og re-etableringsstyring

Håndteres i Kontrakten.

18. Overensstemmelse

Formål

Overholdelse af lovbestemte og kontraktlige krav skal fremgå af Leverandørens sikkerhedspolitik eller procesdokumentation.

Den samlede dokumentation skal synliggøre, at Leverandøren overholder sikkerhedskrav i lovgivningen anført i Kontrakten, herunder:

- Lov om behandling af personoplysninger (Persondataloven) Lov nr. 429 af 31.5.2000 med ændringer, herunder ved lov nr. 280 af 25.4.2001 (Justitsministeriet/Datatilsynet), og Lov nr. 639 af 12.6.2013 (Justitsministeriet).
- Bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Samt at indgåede kontraktlige forpligtelser vedrørende sikkerhed og lovgivning styres og overholdes i forbindelse med Leverandørens opfyldelse af Kontrakten.

Leverandøren skal sikre overholdelse af kravene til sikkerhed i nærværende dokument samt retningslinjerne i ISO 27001:2013 standarden eller tilsvarende.

Revisionskrav og revisionshandlinger i forbindelse med drift af Systemet fremgår af Kontrakten.

Retningslinjer

Leverandøren har udarbejdet retningslinjer og procedurer, som sikrer overensstemmelse med lovgivningen og sikkerhedskrav anført i Kontrakten.

Leverandøren sikrer, at KOMBITs sikkerhedspolitik overholdes, og at sikringsforanstaltninger bliver implementeret og fungerer med den tilsigtede effekt. Fastholdelse af det krævede sikkerhedsniveau er en kontinuerlig proces, hvor opfølgningen tager udgangspunkt i nærværende dokument.

Leverandøren skal være til rådighed for revision/inspektion fra KOMBIT eller dennes repræsentant.

Revisionskrav og handlinger, der involverer kontrol af Systemet i drift hos Leverandøren er nøje planlagt og aftalt for at minimere risikoen for forstyrrelser af de øvrige forretningsaktiviteter. For at forhindre misbrug ved anvendelse af revisionsværktøjer, er adgangen forhindret til udviklingsmiljøer og Driftsmiljøet.

Kontrolmål:

18.1.1 Identifikation af gældende lovgivning og kontraktkrav

Identifikation af gældende lovgivning og kontraktkrav		
KPI-18.1.1.	**Formål:**	Leverandøren skal overholde lovgivningen samt sikkerhedskrav anført i Kontrakten. Overholdelsen skal være dokumenteret og holdes opdateret
	Målepunkt:	2, jf. nedenfor.
	Tærskel:	Overholdelse af lovgivningen og sikkerhedskrav anført i Kontrakten skal være dokumenteret og vedligeholdt.

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Leverandøren har ikke en formaliseret procedure for at identificere sikkerhedskrav i lovgivning og Kontrakten.
1	**Ad hoc / intuitiv**	Leverandøren har ikke en formaliseret procedure for at identificere sikkerhedskrav i lovgivning og Kontrakten, men disse identificeres ad hoc.
2	**Defineret**	Leverandøren har en formaliseret procedure for at identificere sikkerhedskrav i lovgivning og Kontrakten. Relevante medarbejdergrupper er bekendte med denne procedure og følger den.
3	**Styret og målbar**	Leverandøren har en formaliseret procedure for at identificere sikkerhedskrav i lovgivning og Kontrakten. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Der foretages løbende opfølgning på overholdelse af sikkerhedskrav og afvigelser rapporteres.
4	**Optimeret**	Leverandøren har en formaliseret procedure for at identificere sikkerhedskrav i lovgivning og Kontrakten. Relevante medarbejdergrupper er bekendte med denne procedure og følger den. Der foretages løbende opfølgning på overholdelse af sikkerhedskrav og afvigelser rapporteres. Sikringsforanstaltninger implementeres på baggrund af ændrede sikkerhedskrav.

18.2.1 Uafhængig gennemgang af informationssikkerhed

Uafhængig gennemgang af informationssikkerhed		
KPI-18.2.1.	**Formål:**	Leverandørens metode til styring af informationssikkerhed og implementeringen heraf (det vil sige kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) skal gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.
	Målepunkt:	3, jf. nedenfor.
	Tærskel:	Der må ikke afdækkes kritiske, alvorlige eller betydende sikkerhedssvagheder

Nedenstående skema indeholder en beskrivelse af målepunkt 0-4:

0	**Ikke-eksisterende**	Der foretages ikke uafhængig gennemgang af informationssikkerhed hos Leverandøren.
1	**Ad hoc / intuitiv**	Uafhængig gennemgang af informationssikkerhed foretages ad hoc og ikke i henhold til et fastlagt tidsinterval.
2	**Defineret**	Der er en procedure, der sikrer, at uafhængig gennemgang af informationssikkerheden gennemgås med planlagte mellemrum eller ved væsentlige ændringer. Eventuelle svagheder rapporteres og adresseres af Leverandøren inden for et fastlagt tidsinterval.
3	**Styret og målbar**	Der er en procedure, der sikrer, at uafhængig gennemgang af informationssikkerheden gennemgås med planlagte mellemrum eller ved væsentlige ændringer. Eventuelle svagheder rapporteres og adresseres af Leverandøren inden for et fastlagt tidsinterval. Antallet af sikkerhedssvagheder måles over tid, og der udarbejdes handleplaner for håndtering og udbedring af svaghederne.
4	**Optimeret**	Der er en procedure, der sikrer, at uafhængig gennemgang af informationssikkerheden gennemgås med planlagte mellemrum eller ved væsentlige ændringer. Eventuelle svagheder rapporteres og adresseres af Leverandøren inden for et fastlagt tidsinterval. Antallet af sikkerhedssvagheder måles over tid, og der udarbejdes handleplaner for håndtering og udbedring af svaghederne. Leverandøren arbejder proaktivt med at minimere sikkerhedssvagheder.