Skabelon for tjekliste ift. leverandøraftaler

Dette er en skabelon til understøttelse og dokumentation af vurderingen af dækningsgraden for en leverandør, som indgår i organisationens IT/OT-landskab, og understøtter organisationens beredskab eller på anden vis indgår i forsyningskædesikkerhed for organisationen. For hver leverandør inkl. SaaS leverandører udfyldes denne tjekliste. Resultatet fungerer herefter som input til risikovurdering af den pågældende leverandør.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* IT-sikkerhedspolitik
* IT-sikkerhedshåndbog
* Leverandørsikkerhedsprocedure
* Nærværende leverandør tjekliste
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Skabelonerne for de øvrige dokumenterne kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

Tjekliste ift. leverandøraftaler

[Vejledning: Aftale gennemgang bør foretages med jævne mellemrum, for at sikre at aftalen stadig er dækkende og fyldestgørende. Vi anbefaler én gang årligt.]

Tjeklisten giver input til risikovurdering af leverandøren, leverandørensservice og den indgåede aftale. For punkter der ikke er relevante for den pågældende leverandør noteres ”ikke relevant” og en begrundelse i Beskrivelsesfeltet.

|  |  |  |  |
| --- | --- | --- | --- |
| Leverandør: | navn | Aftale indgået: | dato |
| Gennemgang foretaget: | Dato / udført af | Vurdering af leverandørens kritikalitet | Lav / middel / høj |
| Beskrivelse af aftalens formål: |  | [ ]  Databehandler [ ]  NIS2/CER |

|  |  |
| --- | --- |
| Kommunikation til leverandør[ ]  Kontaktpunkt [ ]  Kontakttider | Beskrivelse[Vejledning: Her beskrives om der er aftalt kontaktpunkt i forbindelse med support, og i hvilke tidsperioder der er support, samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov.] |
| Kommunikation fra leverandør[ ]  Kommunikationskanal[ ]  Informationsniveau[ ]  Tidsfrister[ ]  Opsamling efter hændelse og indrapportering til myndigheder | Beskrivelse[Vejledning: Her beskrives om der er aftalt en kommunikationskanal for leverandørens kommunikation til organisationen, hvad der er aftalt af informationer (fx er det dækkende ift. input til hændelseslog i en beredskabssituation), og hvilke tidsfrister der er aftalt (er der aftale om hvor hurtigt og hvor ofte der skal informeres), samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov.] |
| Aftalt serviceniveau[ ]  Vedligehold og opdateringer[ ]  Gendannelses-procedurer[ ]  Gendannelses-prioriteter[ ]  Service Level Aftaler | Beskrivelse[Vejledning: Her beskrives hvad der er aftalt ift. gendannelse af systemer og data, samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov.] |
| Tredjeparter [ ]  Underleverandører[ ]  Myndigheder[ ]  Samarbejdspartnere | Beskrivelse[Vejledning: Her beskrives hvad der er aftalt ift. brug af underleverandører og deres input i en krisesituation, evt. forpligtigelser, som leverandøren har overfor myndigheder og samarbejdspartnere, samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov.Beskriv desuden afhængigheder og en risikovurdering af den pågældende tredjeparts involvering.] |
| Datahåndtering[ ]  Omfang & klassifikation[ ]  Databehandleraftale (persondata)[ ]  Aftale om anden type data[ ]  Ejerskab af data | Beskrivelse[Vejledning: Her beskrives hvis leverandøren databehandler på vegne af organisationen, samt begrundelse for hvorvidt der er indgået dækkende aftaler for databehandlingen.Det skal fremgå af aftalen at I bibeholder ejerskab af data.] |
| Internationale forhold[ ]  Hjemsted / produktionsland[ ]  Underleverandører[ ]  Myndigheder[ ]  Samarbejdspartnere | [Vejledning: Her beskrives hvor leverandøren geografisk er placeret med relevans for service leveret, inkl. hvad der er aftalt ift. brug af underleverandører og deres placering.] |
| Tilsyn[ ]  Certificeringer[ ]  Ekstern revision [ ]  Organisationens audit af leverandør[ ]  Tidsfrister | Beskrivelse[Vejledning: Her beskrives hvordan der føres tilsyn med leverandørens overholdelse af aftalen, samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov.] |