Skabelon for tjekliste ift. IT/Ot-leverandør-aftaler

Dette er en skabelon til understøttelse og dokumentation af vurderingen af dækningsgraden for en IT/OT-leverandør som indgår i organisationens IT/OT-landskab og derfor skal understøtte organisationens krav til IT-sikkerhed. For hver leverandør som understøtter organisationens IT eller OT 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
* IT/OT-leverandør sikkerhedspolitik
* Nærværende IT/OT-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. aftaler med
IT/Ot-leverandører

|  |  |  |  |
| --- | --- | --- | --- |
| Leverandør: | navn | Aftale indgået: | dato |
| Gennemgang foretaget: | Dato / udført af | [ ]  Databehandler [ ]  NIS2 |

|  |  |
| --- | --- |
| Kommunikation til leverandør[ ]  Kontaktpunkt [ ]  Kontakttider | BeskrivelseHer 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 | BeskrivelseHer 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 | BeskrivelseHer 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 | BeskrivelseHer 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. |
| Persondata[ ]  Omfang & klassifikation[ ]  Databehandleraftale | BeskrivelseHer beskrives hvis leverandøren databehandler på vegne af organisationen, samt begrundelse for hvorvidt der er indgået dækkende aftaler for databehandlingen. |
| Tilsyn[ ]  Certificeringer[ ]  Ekstern revision [ ]  Organisationens audit af leverandør[ ]  Tidsfrister | BeskrivelseHer beskrives hvordan der føres tilsyn med leverandørens overholdelse af IT-sikkerhedskrav, samt begrundelse for hvorvidt dette er dækkende ift. organisationens behov. |