

10. Tjekliste for ophør af samarbejde

www.cyber-smv.dk



Ophør af samarbejde
Termination of cooperation

Formål, deltagere og anvendelse

- **Formål**

- Ved ophør af et partnerskab eller en serviceaftale er det vigtigt at tage højde for en række cybersikkerhedstiltag for at beskytte data, systemer og forretningskritiske oplysninger.

- **Deltagere**

- Ledelse, IT, jura.

- **Anvendelse**

- I forbindelse med ophør af samarbejde med samarbejdspartnere (f.eks. leverandører).

Procedure / tjekliste (1/6)

1. Forberedelsesfasen

- **Formål:** Sikre planlægning og overblik før ophøret.
 - ☐ Identificér alle systemer, data og tjenester, som partneren har haft adgang til.
 - ☐ Gennemgå kontrakten for krav om datasletning, fortrolighed og overdragelse.
 - ☐ Udpeg ansvarlige personer for ophørsprocessen (IT, jura, ledelse).
 - ☐ Udarbejd en detaljeret ophørsplan med tidslinje og milepæle.
 - ☐ Informér relevante interne interessenter.

Procedure / tjekliste (2/6)

2. Adgangsstyring

Formål: Forhindre uautoriseret adgang efter ophør.

- ☐ Deaktiver eller fjern alle brugerkonti tilhørende partneren.
- ☐ Skift adgangskoder til fælles konti og systemer og opdater multifaktorautentificering.
- ☐ Luk VPN-, API- (Application Programming Interface) og fjernadgange.
- ☐ Fjern partnerens enheder fra netværk og eventuelle mobile løsninger (mobil, pc).

Procedure / tjekliste (3/6)

3. Datahåndtering

Formål: Beskytte og kontrollere data i overensstemmelse med GDPR og kontrakt.

- ☐ Identificér alle data, som partneren har behandlet eller opbevaret.
- ☐ Aftal og dokumentér, hvordan data skal returneres, overdrages eller slettes.
- ☐ Dokumentér sletningen og få skriftlig bekræftelse på datasletning fra partneren.
- ☐ Gennemfør intern kontrol for at sikre, at ingen data er blevet kopieret eller eksfiltreret.
- ☐ Udarbejd en detaljeret ophørsplan, som beskriver:
 - ☐ Hvilke systemer og data der skal overdrages eller slettes.
 - ☐ Tidsplan for ophør.
 - ☐ Ansvarsfordeling.
 - ☐ Osv.

Procedure / tjekliste (4/6)

4. Dokumentation og overdragelse

Formål: At sikre kontinuitet og overførsel af viden.

- ☐ Modtag al relevant dokumentation (systemopsætning, kildekode, licenser, mv.).
- ☐ Gennemfør en teknisk overdragelse, hvis partneren har stået for drift eller udvikling.
- ☐ Arkivér al kommunikation og dokumentation relateret til ophøret.

Procedure / tjekliste (5/6)

5. Overvågning og hændeshåndtering

Formål: Forebygge og opdage sikkerhedsbrud.

- ☐ Øg overvågning af systemer i overgangsperioden.
- ☐ Gennemfør en sikkerhedsrevision efter ophøret.
- ☐ Vær opmærksom på potentielle trusler, inkl. insidertrusler, og forsøg på datatyveri.
- ☐ Opdater hændeshåndteringsplanen med scenarier relateret til ophør.
- ☐ Hav en beredskabsplan klar i tilfælde af sikkerhedsbrud.

Procedure / tjekliste (6/6)

6. Evaluering og læring

Formål: Forbedre fremtidige processer.

- ☐ Evaluer hele ophørsprocessen med relevante teams.
- ☐ Opdater interne politikker og procedurer baseret på erfaringer.
- ☐ Dokumentér forbedringsforslag til fremtidige samarbejder.
 - ☐ Eksempelvis at inkludere klare klausuler om cybersikkerhed i kontrakten, herunder:
 - ☐ Krav om datasletning.
 - ☐ Fortrolighedsforpligtelser, der fortsætter efter ophør.
 - ☐ Ret til audit og inspektion.
- ☐ Informér relevante interne parter (IT, jura, ledelse) om ophøret.
- ☐ Uddan medarbejdere i, hvordan de skal håndtere henvendelser fra tidligere partnere.