# **Mall för leverantörsbedömning - Informationssäkerhet och GDPR**

Som en del av vårt arbete med informationssäkerhet och dataskydd ber vi er att fylla i denna bedömningsmall. Syftet är att säkerställa att våra leverantörer uppfyller nödvändiga säkerhetskrav.

Vänligen:

1. Besvara alla frågor så fullständigt som möjligt.
2. Bifoga ytterligare dokument om nödvändigt.
3. Kontakta oss om ni behöver förtydliganden.
4. Underteckna och datera den ifyllda mallen.

Era svar kommer att behandlas konfidentiellt och användas för att utvärdera vår gemensamma säkerhetssituation.

## **1. Allmän information**

* Företagsnamn:
* Kontaktperson:
* E-post:
* Telefon:

## **2. Certifieringar och standarder**

* Har ni några relevanta certifieringar (t.ex. ISO 27001, SOC 2)? Om ja, vilka?
* Följer ni några specifika branschstandarder eller best practices?

## **3. Informationssäkerhetspolicy**

* Har ni en dokumenterad informationssäkerhetspolicy?
* När uppdaterades den senast?
* Hur ofta utbildas personalen i informationssäkerhet?

## **4. Dataskydd och GDPR**

* Hur säkerställer ni efterlevnad av GDPR?
* Har ni utsett ett dataskyddsombud (DPO)? Om ja, ange kontaktuppgifter.
* Hur hanterar ni dataöverföringar utanför EU/EES?

## **5. Incidenthantering**

* Beskriv er process för hantering av säkerhetsincidenter.
* Hur snabbt kan ni rapportera en incident till oss?
* Har ni haft några större säkerhetsincidenter under de senaste 24 månaderna?

## **6. Åtkomstkontroll**

* Hur hanterar ni användaråtkomst och behörigheter?
* Använder ni multifaktorautentisering (MFA)?
* Hur ofta granskas användarrättigheter?

## **7. Nätverkssäkerhet**

* Vilka åtgärder har ni implementerat för att skydda ert nätverk?
* Använder ni kryptering för dataöverföring?
* Hur ofta utför ni sårbarhetsanalyser och penetrationstester?

## **8. Fysisk säkerhet**

* Beskriv de fysiska säkerhetsåtgärder ni har implementerat.
* Hur säkras tillgången till era datacenters eller serverlokaler?

## **9. Backup och återställning**

* Hur ofta tar ni backup av data?
* Var lagras backuper och hur skyddas de?
* Hur lång tid tar det att återställa data vid behov?

## **10. Underleverantörer**

* Använder ni några underleverantörer för att behandla våra data?
* Om ja, hur säkerställer ni att de uppfyller samma säkerhetskrav?

## **11. Kontinuitetsplanering**

* Har ni en dokumenterad kontinuitetsplan för verksamheten?
* Hur ofta testas och uppdateras denna plan?

## **12. Datalagringstid och radering**

* Hur länge lagrar ni data?
* Vilka processer har ni för säker radering av data?

## **13. Övervakning och loggning**

* Vilka system och aktiviteter övervakar ni?
* Hur länge sparas loggar?
* Hur skyddas loggarna från manipulation?

## **14. Utveckling och underhåll**

* Hur integrerar ni säkerhet i er utvecklingsprocess?
* Hur hanterar ni säkerhetsuppdateringar och patchar?

## **15. Compliance och revision**

* Genomför ni regelbundna interna eller externa säkerhetsrevisioner?
* Hur hanterar ni resultat och rekommendationer från dessa revisioner?

## **16. Försäkringar**

* Har ni en relevant ansvarsförsäkring som täcker cybersäkerhetsincidenter?

## **17. Övriga kommentarer**

* Finns det något annat ni vill tillägga angående er hantering av informationssäkerhet och dataskydd?

Datum för ifyllnad: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Underskrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Namn och titel: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_