

## 2. Cybersikker- hedsroller og ansvarsområder

[www.cyber-smv.dk](http://www.cyber-smv.dk)



**Roller og ansvar**  
Roles and responsibilities

# Formål, deltagere og anvendelse

- **Formål**

- At understøtte fastlæggelsen, kommunikationen og koordineringen af cybersikkerhedsroller og ansvarsområder for leverandører, kunder og samarbejdspartnere.

- **Deltagere**

- Data-/IT-ansvarlige, leverandører, evt. kunder og andre eksterne relevante samarbejdspartnere.

- **Anvendelse**

- Bør udføres med en passende frekvens.

# Fremgangsmåde

1. Fastlæg roller og ansvar.
2. Kommuniker roller og ansvar.
3. Koordiner og samarbejd.
4. Visualiser og dokumenter.

*Der tages højde for særlige SMV-karakteristika*

- Begrænsede IT-ressourcer.
- Afhængighed af eksterne IT-leverandører.
- Behov for omkostningseffektive sikkerhedsløsninger.

# Fastlæggelse af roller og ansvar (eksempel)

| Rolle                      | Ansvar                                           | Internt / Eksternt | Eksempler                                             |
|----------------------------|--------------------------------------------------|--------------------|-------------------------------------------------------|
| CISO / IT-ansvarlig        | Overordnet cybersikkerhedsstrategi og politikker | Internt            | Udarbejdelse af politikker, risikovurdering           |
| Systemadministrator        | Teknisk implementering og vedligeholdelse        | Internt            | Firewall, adgangskontrol, opdateringer                |
| Databehandler (leverandør) | Sikring af data i overensstemmelse med kontrakt  | Eksternt           | Hosting, cloud-tjenester                              |
| Kunde                      | Overholdelse af sikker brug og rapportering      | Eksternt           | Brug af sikre adgangskoder, rapportering af hændelser |
| Samarbejdspartner          | Overholdelse af fælles sikkerhedsprotokoller     | Eksternt           | Fælles adgang til systemer, datadeling                |

# Kommunikation af roller og ansvar

## Internt

- Politikker og procedurer: Dokumentér og del via intranet eller medarbejderhåndbog.
- Workshops og awareness træning: Regelmæssige sessioner om cybersikkerhed.
- Incident response plan: Klare kontaktpunkter og eskalationsveje.

## Eksternt

- Kontraktuelle aftaler: SLA'er (service level agreements) og databehandleraftaler med sikkerhedskrav.
- Onboarding pakker: Informationsmateriale til nye kunder og partnere.
- Sikkerhedskommunikation: Brug af sikre kanaler til deling af følsomme oplysninger.

# Koordinering og samarbejde

## Internt

- **Tværfunktionelle teams:** IT, HR, ledelse og jura samarbejder om sikkerhed.
- **Regelmæssige møder:** Status på trusler, hændelser og compliance.

## • Eksternt

- **Fælles beredskabsplaner:** Koordineret respons ved sikkerhedshændelser.
- **Sikkerhedsrevisioner:** Gensidige audits og kontroller.
- **Deling af trusselsinformation:** F.eks. via hændelses informationscentre eller branchefora.

# Visualisering og dokumentation (eksempel)

- Der kan med fordel udarbejdes et **RACI-diagram** (Responsible, Accountable, Consulted, Informed) for hver vigtig cybersikkerhedsaktivitet).
- Se eksempel nedenfor.

| Aktivitet         | IT-ansvarlig | Leverandør | Kunde | Partner |
|-------------------|--------------|------------|-------|---------|
| Adgangsstyring    | R            | A          | I     | I       |
| Databeskyttelse   | A            | R          | I     | C       |
| Incident response | A            | C          | I     | C       |
| XX                | XX           | XX         | XX    | XX      |