NOTAT

Kommissorium informationssikkerhedsudvalg

Medlemmer
Informationssikkerhedsudvalget består af:

Rolle	Navn	Funktion
Formand for sikkerhedsudvalget og direktionsrepræsentant		Kommunaldirektør eller direktør for xxxxx
Sekretær for udvalget		Informationssikkerhedskoordinator
Rådgiver for informationssikkerhedsudvalget		Databeskyttelsesrådgiver (DPO)
Chef for xxxxxx og stedfortræder for formanden		
Chef for IT/Digitalisering		
xxxxxxxxxxxxx		
xxxxxxxxxxxxx		

Udvalgets rolle og ansvar

- Har ansvaret for styring af informationssikkerheden i samarbejde med informationssikkerhedskoordinatoren.
- Sætter mål for informationssikkerheden, der er afstemt efter kommunens valgte strategi og risikoniveau og sørger for at informationssikkerheden realiseres og efterleves i organisationen.
- Sikrer at beslutninger bygger på et afvejet helhedssyn – en balance mellem informationssikkerhed, brugervenlighed og økonomi. Det er væsentligt at indsatsen er proportionel med truslerne for organisationen.
- Sikrer at der er udpeget data- og systemejere, samt at fysiske informationsarkiver ligeledes har et ejerskab.
- Sikrer at der foreligger retningslinjer for ejernes ansvar.
- Sikrer at de data- og systemansvarlige samt ejerne af de fysiske informationsarkiver udarbejder de nødvendige procedurebeskrivelser og dokumentation.
- Sikrer uddannelse og oplysning til kommunens medarbejdere om informationssikkerhed.
- Sikrer udarbejdelse af beredskabs-, nød- og reetableringsplaner for informationssikkerhed.
- Sikrer at der mindst en gang årligt gennemføres test af beredskabet for informationssikkerhed.
- Sikrer at sikkerhedsarbejdet har ledelsens opbakning.
  I praksis kan dette ske ved at et af direktionens medlemmer er repræsenteret i informationssikkerhedsudvalget. Alternativt kan der i stedet ske en kvartalsvis rapportering til direktionen.
- Formanden har mandat til at godkende procedurer, politikker, planer mv. vedrørende informationssikkerhedsarbejdet.

NOTAT

Udvalgets opgaver

- Fastlægger informationssikkerhedspolitikkens organisatoriske rammer, ansvarsfordeling og retningslinjer for kontrol og beredskab.
- Fastlægger samt godkender organisationens risikoniveau gennem godkendelse af risikovurderingernes resultater og risikohåndteringsplaner, herunder de accepterede økonomiske risici.
- Reviderer informationssikkerhedspolitikken med udgangspunkt i den aktuelle risikovurdering for organisationen.
- Godkender de underliggende politikker/retningslinjer for sikkerhedsarbejdet, som konkretiserer informationssikkerhedspolitikken, og træffer afgørelse om fortolkning eller ændringer af retningslinjer.
- Evaluerer håndtering af og baggrund for eventuelle angreb og brud på informationssikkerheden (hændelseshåndtering).
- Behandler og godkender kvartalsvis sikkerhedsstatus, herunder status på risikovurdering og andre gennemførte kontroller/opfølgninger i årshjulet.
- Behandler og godkender status på sikkerhedsarbejdet/sikkerhedsprojekter, herunder løbende forbedringer på tekniske foranstaltninger ift. cybersikkerhed (kan være udvalgte områder, så som antivirus, firewall, antispam og -phishing filtre, kryptering, netværkssikkerhed, fysisk sikkerhed.)
- Evaluerer halvårligt gennemførsel af overordnet information om og uddannelse i informationssikkerhed (Awareness)
- Evaluerer intern informationssikkerhedsaudit

Møder i informationssikkerhedsudvalget

Mødes 4 gange årligt.
Der skal foreligge mødekalender for tidspunkt og mødested et halvt år frem i tiden.

Dagsorden

- Godkendelse af referat fra sidste møde
- Status på igangværende arbejder
- Hændelsesrapportering
- Input fra opgaver i årshjulet
- Fastlæggelse af opgaver for det kommende kvartal
- Godkendelse af nye eller opdaterede politikker/vejledninger
- Behandling af rapportering til direktionen (1-4 gange årligt)
- Eventuelt