

### Nr. 1: Cyber- og Informationssikkerhed

	2025	2026	2027	2028
<b>I alt</b>	3.920.000	3.946.000	3.325.000	3.325.000

#### Resume:

Opgradering af systemindkøb samt ressourcer til cyber- og informationssikkerhedsområderne fra 2024 for at opnå et nødvendigt sikkerhedsniveau i Svendborg Kommune svarende til øgede krav og trusselsbilledet i samfundet.

#### Sagsfremstilling:

Cybersikkerhedstrusler mod danske kommuner udgør i dag en stor national bekymring. Kommunerne håndterer store mængder følsomme data i form af personlige oplysninger om borgerne, økonomiske forhold for kommunen og vigtige data relateret til infrastruktur og service, hvorfor sikre stabile IT-systemer er en grundsten for kommunens effektive drift.

I de senere år er cybersikkerhedstruslen blevet endnu mere akut, i form af en stigning i sofistikerede angreb fra internationale hackergrupper og aktører, særligt aktuel i forbindelse med den politiske situation i Rusland. Disse angreb udgør en stigende udfordring for kommunerne at modstå, da de er mere komplekse, hyppigere og målrettede end tidligere, og de kan have alvorlige konsekvenser for samfundets stabilitet og sikkerhed.

Af den årsag er det blevet stadig vigtigere for danske kommuner at sikre robuste sikkerhedsforanstaltninger for at beskytte sig mod sådanne trusler, herunder tekniske løsninger som firewall, antivirussoftware og trusseldetekteringssystemer samt træning af medarbejdere.

Det ændrede nationale trusselsbillede ses desuden også ved Datatilsynets markant øgede fokus på og tilsyn af kommunernes efterlevelse af GDPR- og ISO2700x, hvilket har resulteret i en lang række offentlige sager om bøder og påbud for flere kommuner (eksempelvis sagerne vedr. Chromebook og Aula)

Det kommende NIS2 direktiv varsler yderligere skærpelse af kravene. Direktivet har til formål at styrke cybersikkerheden i hele EU ved at etablere fælles standarder og procedurer for beskyttelse af kritisk infrastruktur og digitale tjenester. For kommunerne indebærer dette, at vi skal sikre, at vores it-infrastruktur og digitale tjenester opfylder de krav og standarder, der er fastsat i NIS2-direktivet. Dette inkluderer blandt andet at identificere og vurdere risici, implementere passende sikkerhedsforanstaltninger, rapportere alvorlige sikkerhedsbrud og opretholde et højt niveau af cybersikkerheds- og informationssikkerhedskompetencer og beredskab.

Med de igennem de senere år øgede krav og fremtidsudsigterne er det nødvendigt at Svendborg Kommune afvikler forskellen på kommunens *nuværende status* på området og det *nødvendige niveau* for at kunne imødekomme aktuelle krav.

Efterlevelse af kravene handler ikke kun om at beskytte sig mod potentielle cyberangreb, men også om at opretholde tilliden hos borgerne og andre interessenter i vores evne til at beskytte deres data på en pålidelig og etisk vis. Samtidig udgør efterlevelse af kravene det nødvendige sikkerhedsmæssige grundlag for fortsat at kunne ibrugtage nye digitale redskaber som f.eks. AI, yderligere foranlediget af den netop vedtagne [EU AI Act](#), som skal regulere brugen af kunstig intelligens i Europa.

Investeringsbehovet fordeler sig på en række systemindkøb i form af et nødvendigt kvalitetsløft af kommunens IT-løsninger, der kan dæmme op for det stigende antal ransomware-angreb, yderligere styrkelse af kommunens anti-virus programmer med en række muligheder for automatiseringer, samt udvidelse af systemer til at styrke sikkerheden på kommunens PC'er og mobile devices. I tillæg til dette kommer udgifter til yderligere segmenterings initiativer. Udgifterne til denne segmentering vil være i form af engangsudgifter til IT-konsulentunderstøttelse af den komplekse, tekniske proces.

Derudover er der behov for ressourcer i form af faste- og tidsbegrænsede ansættelser for at kunne løfte det nødvendige informationssikkerhedsniveau decentralt. Disse ansættelser skal være med til at understøtte den decentrale forvaltning af system- og dataejerskab gennem efterlevelse af allerede eksisterende krav om risiko- og konsekvensanalyser for nye digitale redskaber, databehandleraftaler, kontrol og afgrænsning af adgang til data i de digitale redskaber, stikprøvekontrol af logs - og lignende foranstaltninger der tidligere ikke tilstrækkeligt har været løftet. Ansættelserne omfatter derfor ressourcebehovet for at kunne *drifte det nødvendige niveau* af informationssikkerhed, men også midlertidige ressourcer for at kunne *opnå det nødvendige niveau*.

På cybersikkerhedsområdet er der centralt behov for 1 medarbejder for at kunne mindske sårbarheden om den daglige overvågning og ikke mindst muligheden for at opruste med nye initiativer og spotte hvor de aktuelle trusler er størst og dermed sikre en stabil drift af kommunens IT platform og bidrage til at systemerne hurtigt kommer i luften igen ved eventuelle angreb.

En forudsætning for sikkerheden på de mobileenheder er en større samlet opgradering af mobiler for at sikre kontinuerlig mulighed for sikkerhedsopdatering af styresystemerne, idet der ses et stigende antal forsøg på smishing (angreb via sms'er). Økonomien til indkøb og løbende udskiftning af mobileenheder, der normalt finansierer løbende køb af mobileenheder, ligger decentralt. Udskiftningen fremhæves i nærværende oplæg da det er forudsætning for effekten af nogle af de oplistede tiltag. Anslået samlet engangsinvestering: 1.050.000 kr.- ca. 1.500.000 kr. afhængig af modelvalg.

I ovenstående beskrivelse af investeringsbehovene tages der forbehold for de hastige ændringer på området. Således kan et initiativ i dag skønnes vigtigt men om kort tid kan et andet område være mere afgørende at sætte ind overfor. Derfor er investeringsbehovet for at imødekomme udviklingsplanen frem til 2026 et øjebliksbillede og hensigtserklæring på det, der bør ske på området.

#### Påvirkning på andre områder:

Cyber- og informationssikkerhed vedrører hele kommunens drift samt beskyttelse af borgernes data mod tyveri og misbrug.

# Budget 2025-28

## Økonomiudvalget

## Temaforslag drift

### Økonomi:

	2025	2026	2027	2028
Drift	+ 4 årsværk til informations-sikkerhed (550.000 kr. årligt pr årsværk)	+ 4 årsværk til informations-sikkerhed (550.000 kr. årligt pr årsværk. 1 årsværk kun frem til 1/8)	+ 3 årsværk til informations-sikkerhed (550.000 kr. årligt pr årsværk)	+ 3 årsværk til informations-sikkerhed (550.000 kr. årligt pr årsværk)
	+ 1 årsværk til cybersikkerhed (550.000 kr. årligt)	+ 1 årsværk til cybersikkerhed (550.000 kr. årligt)	+ 1 årsværk til cybersikkerhed (550.000 kr. årligt)	+ 1 årsværk til cybersikkerhed (550.000 kr. årligt)
	+ 670.000 kr. årligt /systemudgift	+ 670.000 kr. årligt /systemudgift	+ 670.000 kr. årligt /systemudgift	+ 670.000 kr. årligt /systemudgift
	+ 500.000 kr. engangsudgift segmentering	+ 300.000 kr. engangsudgift segmentering		
		+ 455.000 kr. årligt /systemudgift	+ 455.000 kr. årligt /systemudgift	+ 455.000 kr. årligt /systemudgift
<b>I alt</b>	3.920.000	3.946.000	3.325.000	3.325.000

+ = udgift, - = indtægt

### CO2-Konsekvensvurdering:

De foreslåede tekniske foranstaltninger samt ansættelser vurderes ikke at afstedkomme yderligere CO2 konsekvenser.