DIGITALISERINGSSTYRELSEN

Vejledning i politikker for informations-sikkerhed

August 2021

2021

Indholdsfortegnelse

Formålet med denne vejledning er at give et overblik over de politikker, der bør udarbejdes og løbende vedligeholdes i forbindelse med implementering og drift af et ledelsessystem for informationssikkerhed (ISMS). I vejledningen beskrives det hvad en informationssikkerhedspolitik er, dennes relation til andre politikker og der gives desuden råd til det praktiske arbejde med selv at formulere en informationssikkerhedspolitik.

Vejledningen er til dig, der har ansvaret for informationssikkerheden i din organisation. Du kunne fx være informationssikkerhedskoordinator, leder med ansvar for informationssikkerhed eller medarbejder på sikkerhedsområdet.

Her kan du læse mere: Skabelon til informationssikkerhedspolitik

1. Hvad er en informationssikkerhedspolitik?

Et ledelsessystem for informationssikkerhed (også benævnt 'ISMS', Information Security Management System) indbefatter alle de politikker, procedurer, retningslinjer og tilhørende ressourcer og aktiviteter, som en organisation administrerer for at beskytte sine informationsaktiver. En central del af ledelsessystemet er *informationssikkerhedspolitikken*, der udstikker linjerne for forretningens prioriteter, og dermed sætter rammen for, hvordan det daglige arbejde med at styre informationssikkerheden skal tilrettelægges. ISO 27002 uddyber, at informationssikkerhedspolitikken bør understøttes af emnespecifikke underpolitikker, som supplerer styringen af sikkerheden i organisationen[1]. Disse underliggende politikker kan udarbejdes, så de relaterer sig til specifikke målgrupper og/eller dækker relevante sikkerhedsområder. De underliggende informationssikkerhedspolitikker vil derfor typisk være mere konkrete og handlingsanvisende end den overordnede informationssikkerhedspolitik.

Hvorfor udarbejde en informationssikkerhedspolitik? Af mindst tre grunde. Dels fordi ISO 27001 stiller krav om, at der udarbejdes en overordnet informationssikkerhedspolitik samt underpolitikker efter behov (ISO 27001 afsnit 2.5 samt afsnit 5.1.1 i ISO 27002). Dels bruges informationssikkerhedspolitikken også ofte til at kommunikere og dokumentere organisationens sikkerhedsniveau til både interne og eksterne parter. Dels kan de indgå som en del af aftalegrundlaget med eksterne parter og anvendes som udgangspunkt for revisioner af selvsamme.

Formålet med denne vejledning er at give et overblik over de politikker, der bør udarbejdes og løbende vedligeholdes som et led i at implementere ISO 27001. I vejledningen beskrives det hvad en informationssikkerhedspolitik er, dennes relation til eventuelle underpolitikker, og der gives råd til det praktiske arbejde med selv at formulere en informationssikkerhedspolitik.

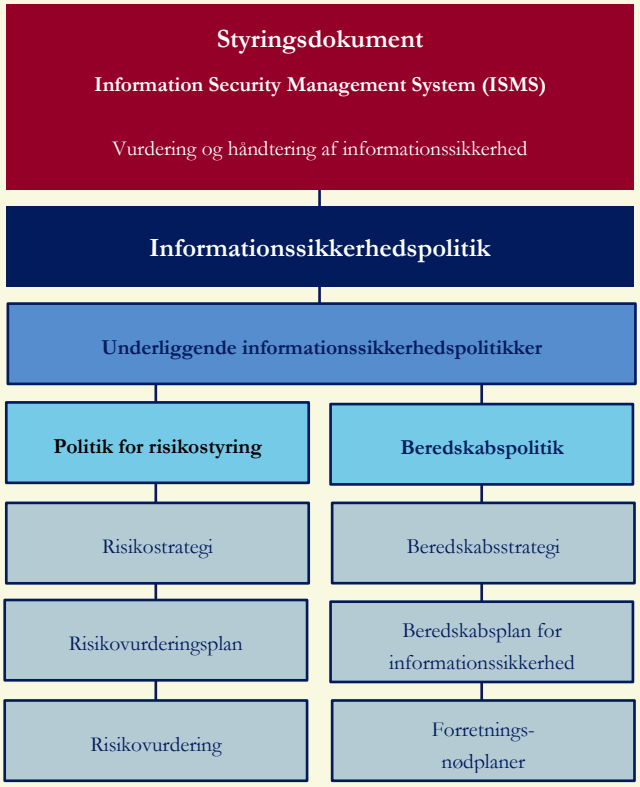
[1] Jf. ISO 27002 afsnit 5.1.1 anvender nogle organisationer andre termer for disse dokumenter som fx "standarder", "direktiver" eller "regler".

2. Overordnet politik og underpolitikker/retningslinjer

Inden man går i gang med at udarbejde informationssikkerhedspolitikken og tilhørende underpolitikker, skal det overvejes, hvilke mål hver enkelt politik skal opfylde. Man kan med fordel grafisk skitsere den ønskede dokumentstruktur og beskrive formålet med de enkelte dokumenttyper og deres indbyrdes relation.

For at skabe en god samlet struktur der både indeholder den overordnede informationssikkerhedspolitik og de underliggende politikker (nogle gange benævnes underpolitikker også 'retningslinjer'), kan udarbejdes særlige emner, som de underliggende politikker tilknyttes/retningslinjer, som det ses i eksemplet nedenfor.

Figur 1
Eksempel på dokumenthierarki



Kilde: Digitaliseringsstyrelsen

Informationssikkerhedspolitikkerne skal altid tilpasses organisationen og dens forretningsområde, it-anvendelse og eksisterende styringsmekanismer. Når informationssikkerhedspolitikkerne udarbejdes, er det derfor en god idé at gennemgå organisationens strategi og it-strategi for at sikre, at politikkerne er i overensstemmelse med målsætningerne i organisationen.

Tjekliste:

- ✓ Er målene for informationssikkerhedspolitikken afklaret?
- ✓ Afspejler politikkerne organisationens forretningsstrategi og it-strategi?
- ✓ Har organisationen et særligt forretningsfokus, som informationssikkerhedspolitikkerne bør tage hensyn til, fx organisationens placering i en konkret sektor?
- ✓ Er der særlige eksterne krav, som informationssikkerhedspolitikkerne bør tage hensyn til – interessenters forventninger, lovkrav og andre krav?
- ✓ Er der skabt en hierarkisk struktur for, hvordan den overordnede politik relaterer sig til eventuelle underpolitikker?

3. Struktur for informationssikkerhedspolitikken

ISO 27001 afsnit 5.2 kræver, at informationssikkerhedspolitikken skal:

- Passe til organisationens formål
- Omfatte målsætninger for informationssikkerhed
- Udtrykke en forpligtelse til at opfylde relevante krav ang. Informationssikkerhed
- Udtrykke en forpligtelse til løbende at forbedre sit ledelsessystem for informationssikkerhed
- Være dokumenteret
- Kommunikeres internt, og være tilgængelig for interessenter, hvis hensigtsmæssigt

Som det ses af ovenstående, specificerer ISO 27001 ikke særligt nøje, hvordan en informationssikkerhedspolitik skal se ud. Dette gør sig også gældende for de relevante dele af ISO 27002 (afsnit 5.1.1), der angår informationssikkerhedspolitikken. Der er altså god mulighed for at vælge en struktur, der flugter med organisationens karakter.

På https://sikkerdigital.dk/Media/637963161536561731/informationssikkerhedspolitik.pdf findes en skabelon til en informationssikkerhedspolitik, som kan benyttes til inspiration eller som udgangspunkt. Den nedenfor foreslåede struktur følger skabelonen. Politikken kan fx indeholde følgende elementer:

Indledning
Informationssikkerhedspolitikken bør afspejle organisationen, dens kontekst, relevante lovgivningsmæssige krav og relevante interessenters behov. Her defineres målsætningerne og omfanget af informationssikkerhedsstyringen. Det vil fx være relevant at nævne, hvis det er tilfældet, at også processer hos eksterne it-leverandører er en del af ledelsessystemet.

Informationssikkerhedspolitikken bør angive, hvordan organisationen forholder sig til et styret procesforløb med hensyn til planlægning, implementering, revurdering og forbedring af styringsindsatsen.

Roller og ansvar
ISO 27001 kræver, at ledelsens engagement og involvering i styring af informationssikkerheden er synlig og reel. Ledelsen skal således i informationssikkerhedspolitikken forpligte sig til løbende forbedring af ledelsessystemet. Ledelsen skal sikre, at relevante roller til styring af informationssikkerheden er defineret, og at opgaver og ansvar er beskrevet.

Risikostyring
Sikkerhedsniveauet skal vurderes og besluttes på grundlag af gennemførte risikovurderinger og de planer for minimering, overførsel, eliminering og/eller accept af risici, som vurderingerne viser behov for. Informationssikkerhedspolitikken sætter rammerne for risikovurdering og risikohåndtering. Det bør beskrives i politikken, hvorledes de gennemførte risikovurderinger udmøntes i sikkerhedsmæssige retningslinjer og –processer.

Sikkerhedsbevidsthed
Det er vigtigt, at alle medarbejdere er bekendt med deres ansvar for informationssikkerheden. Det vil derfor være relevant, at informationssikkerhedspolitikken indeholder et afsnit om ledelsens forventninger til medarbejderne

Afvigelser fra informationssikkerhedspolitikken
I nogle tilfælde kan det være rimeligt og relevant ikke at efterleve specifikke krav i politikken, og det bør derfor angives, hvem i organisationen der har bemyndigelse til at fravige fra politikken.

Informationssikkerhedspolitikken angiver de mål og krav til processer, sikringsforanstaltninger mm., som er nødvendige til sikring af organisationens systemer og data til understøttelse af forretnings-kritisk opgaveløsning. Det bør fremgå af politikken, hvis overtrædelse af processer og foranstaltninger kan medføre sanktioner for medarbejdere, der ikke efterlever informationssikkerhedspolitikken eller de underliggende politikker.

Godkendelse og kommunikation
Det bør altid klart og formelt fremgå, at informationssikkerhedspolitikken er godkendt af ledelsen og hvornår dette er sket. Endvidere bør det fremgå, at den skal kommunikeres til alle medarbejdere i organisationen. Det bør også angives hvornår og hvordan informationssikkerhedspolitikken evalueres og opdateres.

Versionshistorik
Ud over ovennævnte information om godkendelse af informationssikkerhedspolitikken, bør følgende også fremgå:

- Version
- Placering
- Forfatter
- Godkendt af
- Gyldighedsdato
- Næste opdatering
- Ændringslog

4. Struktur for de underliggende informationssikkerhedspolitikker/ retningslinjer

Den overordnede informationssikkerhedspolitik bør understøttes af emnespecifikke og underliggende politikker, som definerer implementering af foranstaltninger til styring af risici på et mere konkret niveau. Det kan være med angivelse af de funktioner i organisationen, som er involveret inden for det pågældende område. Politikkerne kan tage udgangspunkt i emnerne i ISO 27002 – som fx adgangsstyring – og i andre tilfælde i helt konkrete kontrolområder såsom 'backup'.

Politikkerne bør målrettes de målgrupper i organisationen, som politikkerne er relevante for.

Figur 2
Eksempel på målgrupper for de underliggende politikker

Politik	Medarbejdere	It-ansvarlige	Ledelse	Leverandører
Informationssikkerhedspolitik	X	X	X	X
Organisering af informationssikker- hed	(X)	(X)	X	
Medarbejdersikkerhed	X	X	X	
Styring af aktiver	(X)	X		X
Adgangsstyring	(X)	X	X	(X)
Kryptografi		X		X
Fysisk sikring og miljøsikring	X	X	X	X
Driftssikkerhed		X		X
Kommunikationssikkerhed	(X)	X		X
Anskaffelse, udvikling og vedligeholdelse af systemer		X	X	X
Leverandørforhold		X	X	X
Styring af informationssikkerheds- brud	(X)	X	X	X
Informationssikkerhedsaspekter ved nød-, beredskabs- og reetablerings- styring		X	X	X
Beredskabsplan	X	X	X	(X)

Kilde: Digitaliseringsstyrelsen

Strukturen i de underliggende informationssikkerhedspolitikker bør afhænge af organisationens måde at kommunikere til medarbejdere på. Politikkerne følge en bestemt struktur med mulighed for at den enkelte målgruppe kan se eget ansvar i forhold til den pågældende politik.

Mulige, generelle indholdselementer i underliggende politikker:

- Politikkens formål
- Målgrupper – angivelse af ansvar
- Generelle forhold – fx noget der gælder for alle
- Specifikke forhold
- Ejerskab og ansvar for politikken
- Succeskriterier – kan være i form af KPI'er (Key Performance Indicators) og/eller KRI'er (Key Risk Indicators)
- Måling og audit – hvordan der følges op på, at politikken efterleves

Vejledning i politikker for informationssikkerhed
Udgivet august 2021
Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
www.sikkerdigital.dk.

Foto Colourbox

ISBN: 978-87-93073-41-8