DIGITALISERINGSSTYRELSEN

Vejledning i informations-sikkerhedspolitik

Februar 2015

Vejledning i informationssikkerhedspolitik

Udgivet februar 2015

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
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox

Elektronisk publikation
ISBN 978-87-93073-10-4

Indhold

1. Hvad er en informations-sikkerhedspolitik?

ISO 27001 beskriver, at informationssikkerhedspolitikken er topledelsens dokument, der fastlægger styringen af informationssikkerheden i organisationen. ISO 27002 uddyber, at den overordnede politik bør understøttes af emnespecifikke politikker, som supplerer styringen af sikkerheden i organisationen. Disse underliggende politikker kan udarbejdes, så de relaterer sig til specifikke målgrupper og/eller dækker relevante sikkerhedsområder. De underliggende informationssikkerhedspolitikker vil derfor være mere konkrete og vil kunne afløse tidligere retningslinjer/procedurer.

Informationssikkerhedspolitikkerne er rammesættende og dermed de mest centrale dokumenter i arbejdet med informationssikkerhed i en organisation. Informationssikkerhedspolitikkerne er først og fremmest et strategisk styringsredskab, hvor organisationens målsætning, afgrænsning, ansvarsplacering og rammer for styringen af arbejdet med informationssikkerhed fastsættes. Informationssikkerhedspolitikkerne kan også bidrage til at skabe en fælles forståelse i organisationen for, hvad informationssikkerhed indebærer, og hvilken tilgang man har til det.

Informationssikkerhedspolitikkerne skal blandt andet

- Passe til organisationens formål, dvs. tage hensyn til forretningsmæssige karakteristika, kontekst, interessenter, aktiver og teknologi
- Omfatte - eller opstille rammer for fastlæggelse af - målsætninger for informationssikkerhed, dvs. skabe en samlet udmelding for retning og principper for styring og handling i forhold til informationssikkerhed
- Forholde sig til forretningsmæssige krav, lov- eller myndighedskrav og kontraktlige forpligtelser vedrørende informationssikkerhed
- Udgøre den del af virksomhedens strategiske risikoledelse, hvor etablering og vedligeholdelse af ISMS'et vil finde sted
- Være rammer for analyse og vurdering af it-risici
- Indeholde en forpligtelse til at opfylde relevante krav til informationssikkerhed
- Indeholde en forpligtelse til vedvarende forbedring af informationssikkerhedsarbejdet
- Godkendes af ledelsen
- Kommunikeres internt til alle medarbejdere og eksternt til relevante parter
- Evalueres med planlagte mellemrum eller efter væsentlige ændringer.

Informationssikkerhedspolitikkerne skal være tilgængelige for alle ansatte i organisationen, så ledelsens målsætninger og baggrund for politikkerne er kendt af medarbejderne. Informationssikkerhedspolitikkerne bruges i mange sammenhænge også til at kommunikere og dokumentere organisationens sikkerhedsniveau til både interne og eksterne parter. De kan samtidig indgå som en del af aftalegrundlaget med eksterne parter og anvendes som udgangspunkt for revisioner mv.

Hvem ejer informationssikkerhedspolitikken?

Normalt det vil det være informationssikkerhedskoordinatoren, som formulerer organisationens informationssikkerhedspolitikker, herunder den overordnede informationssikkerhedspolitik. Den overordnede informationssikkerhedspolitik skal altid godkendes af organisationens øverste ledelse, mens de øvrige politikker vedligeholdes af informationssikkerhedskoordinatoren og godkendes af informationssikkerhedsudvalget.

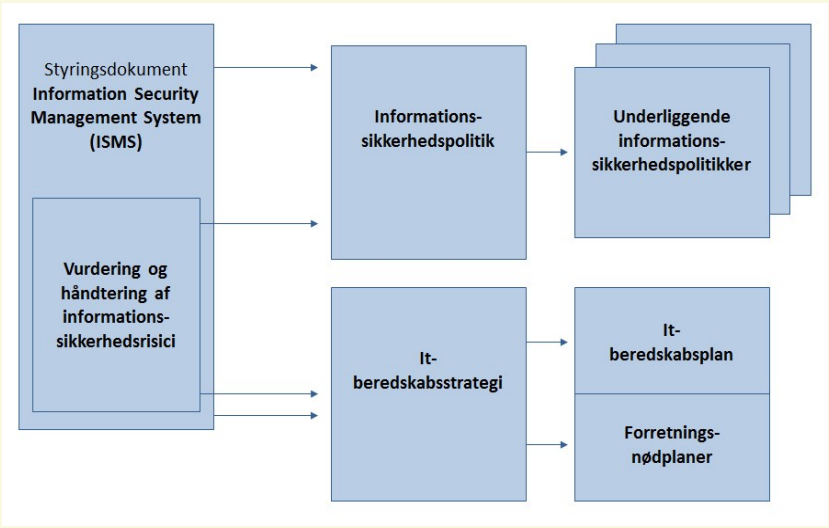
Informationssikkerhedspolitikkerne skal desuden revurderes med planlagte mellemrum. I praksis er det mest hensigtsmæssigt at gøre det i forlængelse af den årlige risikovurdering, så der kan tages højde for væsentlige ændringer i risikobilledet.

2. Relationen til andre politikker og strategier

Inden man går i gang med informationssikkerhedspolitikkerne, skal det overvejes, hvilke konkrete formål de skal opfylde, hvilke andre dokumenter der eventuelt findes - og skal tages hensyn til. Det vigtigste er ikke, hvilke dokumenter der beskriver de forskellige niveauer af sikkerheden, men at sammenhængen og hierarkiet mellem dokumenterne er beskrevet. Man kan med fordel, grafisk eller på anden måde, skitsere den ønskede dokumentstruktur og beskrive formålet med de enkle dokumenttyper og deres indbyrdes relation.

For at sikre sammenhæng mellem den overordnede informationssikkerhedspolitik og de underliggende politikker kan der eventuelt udarbejdes særlige emner, som de underliggende politikker knyttes op på. På den måde skabes der en rød tråd mellem den overordnede målsætning og den konkrete udmøntning.

Eksempel på dokumenthierarki



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

Politikkerne skal altid afspejle organisationens aktuelle risikobillede, som etableres i de periodisk gennemførte it-risikovurderinger.

Overvejelser til informationssikkerhedspolitikkerne

- 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?

3. Struktur for en overordnet informations-sikkerhedspolitik

Der er ikke formelle krav til, hvordan en overordnet informationssikkerhedspolitik skal udformes, men den kan i sin opbygning tage udgangspunkt i strukturen i ISO 27001 og inddrage andre relevante områder af relevans for den pågældende organisation, herunder lovkrav.

Politikken kan fx indeholde følgende elementer:

Indledning – kontekst og afgrænsning
Den overordnede informationssikkerhedspolitik bør afspejle organisationen, dens kontekst, relevante lovgivningsmæssige krav og interessenter. Her defineres omfanget af styringen af informationssikkerheden. Det vil fx være relevant at nævne, at også processer hos eksterne it-leverandører er en del af ledelsessystemet.

Den overordnede informationssikkerhedspolitik bør angive, hvordan organisationen forholder sig til et styret procesforløb mht. planlægning, implementering, revurdering og forbedring af styringsindsatsen.

Ledelsens ansvar og fokus
ISO 27001 har stærkt fokus på, at ledelsens engagement og involvering i styring af informationssikkerheden er synlig og reel. Ledelsen skal således i den overordnede informationssikkerhedspolitik 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.

It-risikovurdering og -håndtering
Sikkerhedsniveauet skal vurderes og besluttes på grundlag af gennemførte it-risikovurderinger og de planer for minimering, overførsel, eliminering og/eller accept af risici, som vurderingerne viser behov for. Den overordnede informationssikkerhedspolitik sætter rammerne for it-risikovurdering og -håndtering.

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

Dispensation 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.

Brud på informationssikkerheden
Den overordnede informationssikkerhedspolitik angiver de mål og krav til processer, kontroller mm., som er nødvendige til sikring af organisationens systemer og data til understøttelse af forretningskritisk opgaveløsning. Det bør fremgå af politikken, hvis overtrædelse af processer og kontroller kan medføre sanktioner.

Godkendelse og kommunikation
Det bør altid klart og formelt fremgå, at den overordnede informationssikkerhedspolitik er godkendt af ledelsen og hvornår. Endvidere bør det fremgå, at den skal kommunikeres til alle medarbejdere i organisationen.

4. Struktur for de underliggende informationssikkerhedspolitikker

Den overordnede informationssikkerhedspolitik understøttes af emnespecifikke politikker, som definerer implementering af kontroller til styring af it-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 som backup.

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

Eksempel på målgrupper for de underliggende politikker

Politik	Medarbejdere	It	Ledelse	Leverandører
Informationssikkerhedspolitik	X	X	X	X
Organisering af informationssikkerhed	(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 informationssikkerhedsbrud	(X)	X	X	X
Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring		X	X	X
Overensstemmelse	X		X	X

Strukturen i de understøttende informationssikkerhedspolitikker bør i sidste ende afhænge af organisationens måde at kommunikere til medarbejdere på. Under alle omstændigheder bør politikkerne følge en bestemt struktur, med mulighed for at den enkelte målgruppe kan se sig selv og eget ansvar i forhold til den pågældende politik.

Mulige, generelle indholdselementer i understøttende 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 med angivelse af ønsket resultat
- Måling og audit – hvordan følges der op på, at politikken efterleves
- Opfølgning på politikken – hvem følger op