GOD SKIK FOR INFORMATIONSSIKKERHEDSPOLITIK

LinkGRC

A Nordic leader in all aspects of Governance, Risk and Compliance

GOD SKIK FOR INFORMATIONSSIKKERHEDSPOLITIK

Virksomhedens informationssikkerhedspolitik er i sin enkelhed et modsvar til en virksomheds risikoprofil. Med andre ord er en virksomheds risikovurdering en væsentlig forudsætning for at formulere en god og effektiv informationssikkerhedspolitik.

Udformning af informationssikkerhedspolitikken og underliggende forretningsgange kan umiddelbart opfattes som en stor og omkostningstung opgave, der trods sin vigtighed afholder en del virksomheder fra at påbegynde processen.

Nøglen er indledningsvis primært at fokusere på virksomhedens vigtigste risici og udarbejde første udgave af informationssikkerhedspolitikken derefter.

Informationssikkerhedspolitikker er medvirkende til at understøtte virksomhedens produktivitet og effektivitet, og påvirke medarbejderes, partneres og leverandørers adfærd. Formålet er at skabe en sikkerhedskultur, der er naturlig og integreret når virksomhedens opgaver skal løses.

EN GOD START

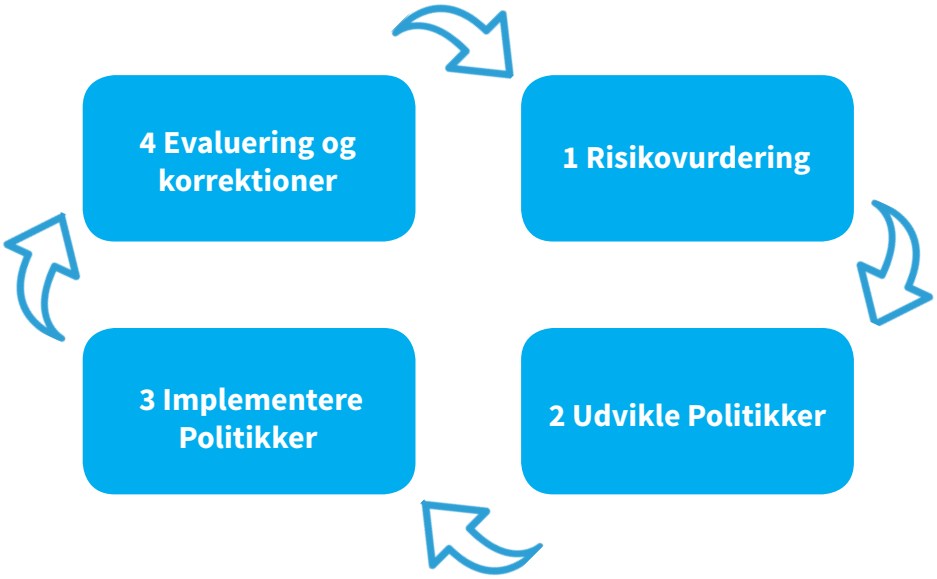
Forankring og planlægning af processen er en væsentlig forudsætning. Virksomhedens ansvarlige for informationssikkerhed skal sikre, at informationssikkerhedspolitikken bliver udviklet, vedligeholdt og implementeret i virksomheden.

UDVIKLING OG VEDLIGEHOLDELSE AF INFORMATIONSSIKKERHEDSPOLITIKKEN

Processen består af 4 hovedaktiviteter.

RISIKOVURDERING; En risikovurdering af virksomhedens IT og generelle forretningsprocesser resulterer i et risiko og trusselsbillede, der danner grundlaget for at udvikle informationssikkerhedspolitikken. Risikovurderingen foretages typisk hvert år, samt hvis der sker væsentlige ændringer i risiko og trusselsbilledet, hvis ny teknologi tages i anvendelse, eller ved større organisatoriske ændringer med konsekvens for informationssikkerheden. Alle ændringer ajourføres i den eksisterende risikovurdering.

GOD SKIK FOR INFORMATIONSSIKKERHEDSPOLITIK



UDVIKLING AF POLITIKKER; Inden arbejdet går i gang med at udarbejde informationssikkerhedspolitikken og underliggende forretningsgange, skal der fastlægges en dokumentstruktur og dokumentskabeloner. Dette skal gøres for at lette identifikation, vedligeholdelse og implementering af politikker og forretningsgange i virksomheden.

IMPLEMENTERING AF POLITIKKER; Sikkerhedspolitikken skal være godkendt af virksomhedens ledelse. Vedtagne politikker og forretningsgange skal udbredes og implementeres i virksomheden. Implementeringen involverer mange parter i virksomheden, og er ikke alene den sikkerhedsansvarliges ansvar. HR funktioner, den generelle ledelse og de funktionsansvarlige har et med- ansvar for at sikre, at medarbejderne er bekendt med politikkernes formål og budskaber. Inkluder kort gennemgang af vigtigste budskaber på introduktionsdage for nye medarbejdere, og gennemfør informationsdage minimum én gang om året for medarbejdere for at sikre de kan huske det væsentligste indhold.

EVALUERING OG KORREKTIONER; Evaluering og korrektioner skal sikre aktualitet og afspejle det faktiske behov for justering af eksisterende politikker og forretningsgange. Når først processen er etableret, skal der planlægges revidering og gengodkendelse igen. Behovet for at revidere politikker og forretningsgange vil typisk være med 1 til 2 års mellemrum.

GOD SKIK FOR INFORMATIONSSIKKERHEDSPOLITIK

HVAD SKAL EN INFORMATIONSSIKKERHEDSPOLITIK INDEHOLDE

En overordnet informationssikkerhedspolitik skal forholde sig til sikkerhedsprincipperne for en række områder og må gerne anvende inspiration fra anerkendte standarder som fx ISO27001/2:2013.

1) Ledelsens retningslinjer for sikkerhed

2) Hvordan arbejdet med sikkerhed organiseres i virksomheden

3) Medarbejdersikkerhed, sikring af utilsigtet og tilsigtet brud på sikkerheden

4) Styring af aktiver, både fysiske og data aktiver

5) Adgangsstyring til applikationer og andre IT ressourcer

6) Behov for kryptografi

7) Fysisk sikkerhed, herunder fysiske arealer og IT udstyr

8) IT drift, ansvar for operationelle procedurer, backup, opdatering af software, virusbeskyttelse mv.

9) Netværk og kommunikationssikkerhed

10) Anskaffelse af systemer, udvikling og vedligeholdelse

11) Leverandørrelationer, påkrævet sikkerhed

12) Styring af hændelser i form af uforudsete nedbrud, fejl eller eksterne forsøg på at stoppe eller hæmme virksomhedens pro duktion og effektivitet

13) Forretningens tilgængelighed, tilpasning af IT miljøet ud fra et forretningsmæssigt behov

14) Overensstemmelse med lovgivning, kontrakt vilkår og internt fastsatte regler

Informationssikkerhedspolitikken suppleres med specifikke forretningsgange og nøglekontroller der er vigtige for virksomheden for at implementere informationssikkerhedspolitikken, og kunne påse at den er implementeret.

Informationssikkerhedspolitikken skal desuden redegøre for konsekvenser ved ikke at følge retningslinjerne og henvise til kommunikationsveje i tilfælde af brud på sikkerheden.

GOD SKIK FOR INFORMATIONSSIKKERHEDSPOLITIK

GODE RÅD

Risikovurdering skal være på plads når informationssikkerhedspolitikken skrives. Anerkendte internationales standarder giver et bud på, hvordan en risikovurdering gribes an som fx ISO31000 eller ISO27005.

Ret indledningsvis fokus mod de vigtigste sikkerhedsemner og undgå udvikling af politikemner og forretningsgange med lav prioritet. For mange politikemner og forretningsgange med lav prioritet pålægger virksomheden et unødigt ressourceforbrug og komplicerer implementeringen.

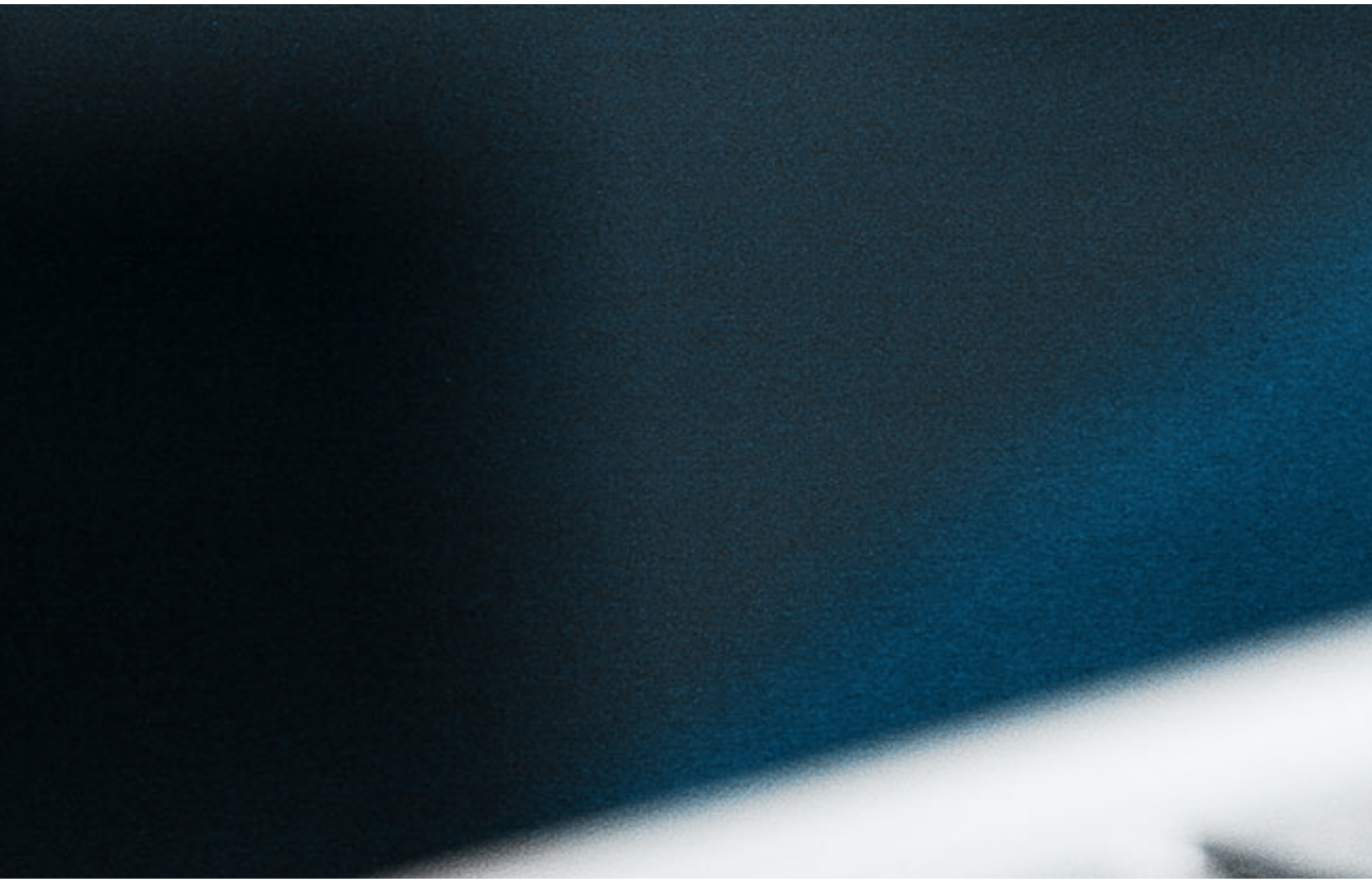
Politikker og forretningsgange skal være realistiske, beskrive nuværende niveau og processer samt undgå for generelle vendinger og krav. De skal være præcise og lette at gå til.

Kend informationssikkerhedspolitikkens modtagergruppe og indret kommunikationen og sprogbruget derefter.

Der er skrevet en del generelle politikker, der passer til mange virksomheders behov. Det kan være et udgangspunkt, men risikoen er, at virksomhedens primære behov ikke bliver indfriet og informationssikkerhedspolitikken mister sin aktualitet og værdi.

Hvis man som virksomhed ikke ønsker af afsætte ressourcer og kompetencer til at foretage en risikovurdering og udarbejde informationssikkerhedspolitikken og forretningsgange, kan det give mening at indlede et samarbejde med en leverandør, der beskæftiger sig med risikostyring og informationssikkerhed.

Vær bevidst om, at ansvaret for sikkerhed i sidste instans påhviler virksomheden selv.



LinkGRC ApS

Jagtvej 223, 4. sal
2100 København Ø

T: +45 7022 3280
@: info@linkgrc.com
W: www.linkgc.com