Ishøj Kommunes Informationssikkerhedspolitik

Godkendt af Byrådet den 06.09.2022

Indholdsfortegnelse

Indledning

Vi lever i et informationssamfund, hvor vi behandler stadigt flere informationer, herunder også følsomme og fortrolige oplysninger om borgere, medarbejdere og organisationen. Samtidig gør udviklingen i vores digitale samfund, at informationen er blevet mere tilgængelig via digitale systemer, og ikke længere kun findes på papir eller som viden i mennesker.

Måden vi arbejder med informationer i dag betyder, at det er blevet langt mere komplekst at beskytte oplysningerne tilstrækkeligt. For at imødekomme den øgede kompleksitet, er der derfor behov for et grundlæggende fundament for arbejdet med informationssikkerhed i Ishøj Kommune, som kan indarbejdes i organisationens daglige arbejdsgange, rutiner og procedurer.

Informationssikkerhedspolitikken er et understøttende styredokument i forhold til kommunens seks hovedpolitikker, og bidrager dermed til det fundament, der skal løfte ambitioner og visioner i hovedpolitikkerne.

Målsætning

Formålet med denne informationssikkerhedspolitik er at sikre, at Ishøj Kommunes følsomme og fortrolige oplysninger altid er beskyttet tilstrækkeligt, så kommunen fortsat fremstår som en troværdig og pålidelig organisation for borgere, samarbejdspartnere og i offentligheden.

Standarder som strategisk fundament

Hensigten med Ishøjs Kommunes informationssikkerhedspolitik er at skabe en ramme for arbejdet med informationssikkerhed, så beskyttelsen af informationer sker efter gældende lovgivning, anerkendte standarder og fastlagte regler. Rammen om arbejdet med informationssikkerhed i Ishøj Kommune er derfor funderet i den internationale standard ISO27001.

ISO 27001 er en international standard for informationssikkerhed, som opstiller et sæt gode spilleregler for arbejdet med informationssikkerhed. Med udgangspunkt i ISO27001 har Ishøj Kommune et stærkt fundament til styring af informationssikkerhed. ISO27001 er således også fundamentet, som vi bygger oven på, når vi skal implementere ny lovgivning eller standarder, som omhandler informationssikkerhed.

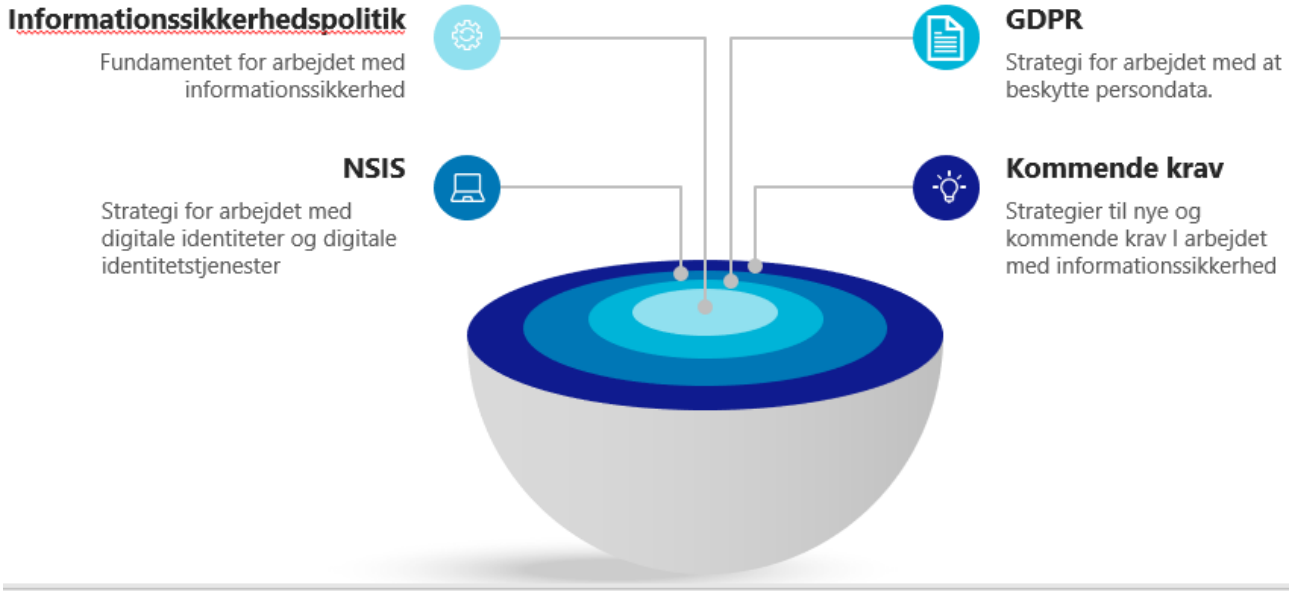
Risikostyring

Kernen i ISO27001 er en systematisk tilgang til risikostyring. En væsentlig del af risikostyringen er risikovurderinger af kommunens IT-systemer og arbejdsgange, hvor formålet er at nedbringe *risikoen* for, at kommunens informationer bliver tilgængelige for uvedkommende (fortrolighed), er forkerte eller ikke opdaterede (integritet) eller bliver utilgængelige ved eks. IT-nedbrud (tilgængelighed).

Arbejdet med informationssikkerhed er en løbende risikostyring, hvor der følges op på risikovurderinger, procedurer og føres interne tilsyn for at sikre, at kommunens behandling af persondata ikke udgør en væsentlig risiko for borgerne eller kommunen selv.

Kernen i informationssikkerhedsarbejdet

ISO27001 udgør derved fundamentet for arbejdet med informationssikkerhed i Ishøj Kommune. Kernen i informationssikkerhedsarbejdet bruges som løftestang til implementering af andre standarder og lovkrav inden for informationssikkerhed, som eksempelvis National Standard for Identiteters Sikringsniveauer (NSIS), GDPR mv. Herved opnår organisationen en fokuseret, optimeret og sammenhængende indsats, med ensartet håndtering af samme krav på tværs af organisationen.



Beredskabsplaner

En væsentlig del af arbejdet med informationssikkerhed er et overblik over, hvilke af kommunens systemer, som er vitale for levering af kritiske ydelser til borgere, virksomheder eller for kommunens drift. I overblikket skal der samtidig være fastsat maksimalt accepteret nedetid (utilgængelighed) på disse systemer.

På de vitale områder skal der være lokale nødprocedurer og beredskabsplaner for, hvordan driften kan sikres i forbindelse med IT-nedbrud. Disse procedurer skal afprøves med passende intervaller, så vi sikrer, at kommunens drift kan fortsætte forsvarligt, hvis IT-systemerne er utilgængelige.

Ansvar for informationssikkerhedspolitikken

Det er Ishøj Kommunes ambition, at kendskabet til og arbejdet med informationssikkerhed er bredt forankret i organisationen således, at informationssikkerhed i det daglige arbejde indgår på lige fod med andre fagligheder.

Informationssikkerhed er et fælles ansvar i Ishøj Kommune, og opgaven kræver, at alle ansatte tager aktiv del i og ansvar for beskyttelsen af borgernes og kommunens data. Alle ansatte og nyansatte der arbejder med personoplysninger gennemgår derfor bl.a. et e-læringskursus i GDPR årligt, så de er klædt på til at løfte denne opgave.

Informationssikkerhedspolitikken kommunikeres ud til alle nuværende og nye ansatte i Ishøj Kommune, og alle ansatte er forpligtet til at efterleve informationssikkerhedspolitikken samt øvrige regler og procedurer på området.

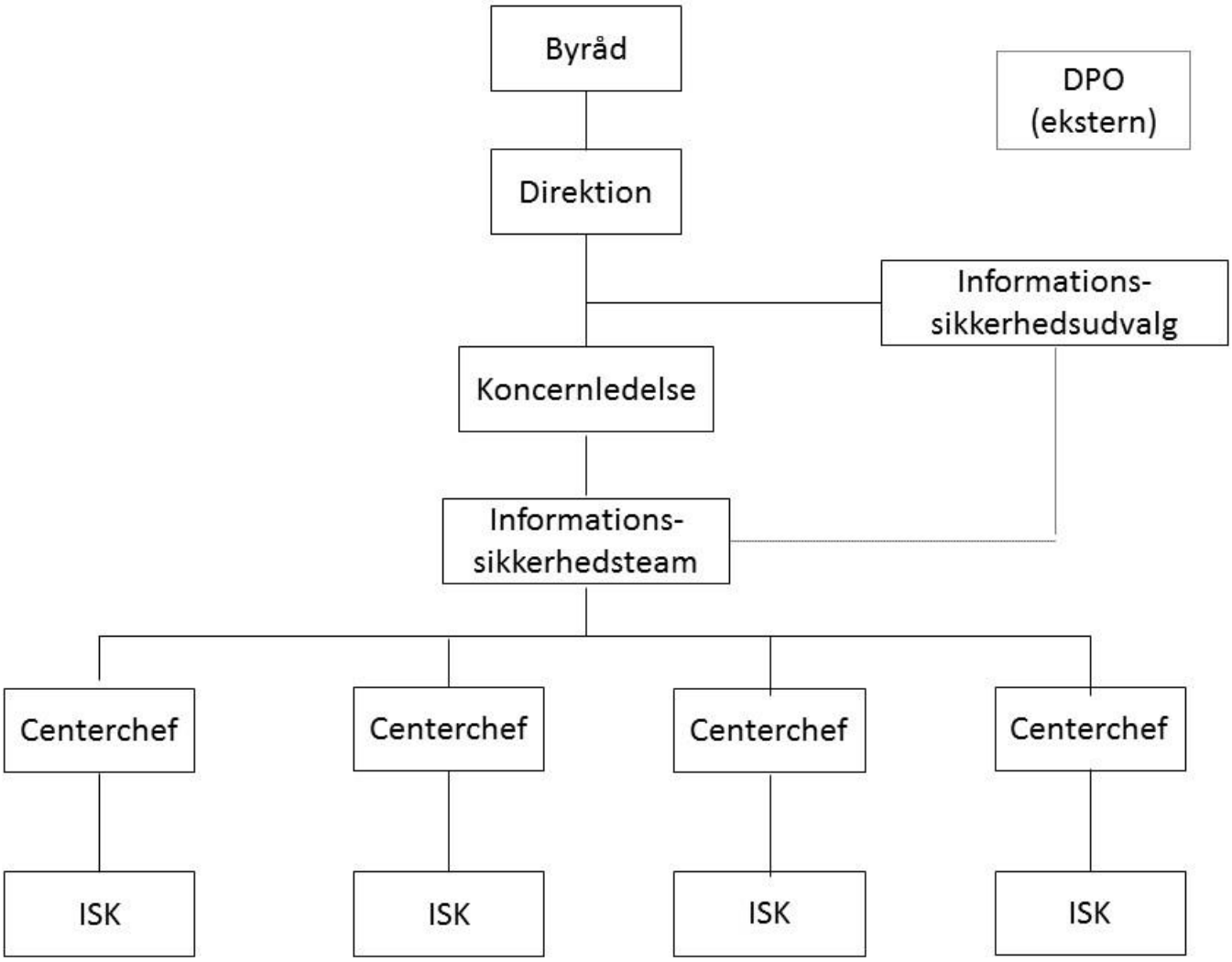
Ansvaret for informationssikkerhedspolitikken er beskrevet i Bilag 1.

Godkendelsesproces

Informationssikkerhedspolitikken skal godkendes af Koncernledelsen og Byrådet og implementeres af organisationen. Politikken skal godkendes årligt.

Bilag 1: Organisation for informationssikkerhed

Arbejdet med informationssikkerhed er forankret i organisationen på forskellige niveauer. Hvert niveau har en rolle med forskellige aktiviteter og tilknyttet ansvar.



**ISK = InformationsSikkerhedsKoordinator*

Byrådet	• Godkender informationssikkerhedspolitikken
Direktionen	• Sammensætter Informationssikkerhedsudvalget og udpeger CISO*. CISO samt leder af informationssikkerhedsteamet er fødte medlemmer af informationssikkerhedsudvalget • Opfølgning på informationssikkerheden i Ishøj Kommune • Informerer Byrådet om relevante emner vedrørende informationssikkerheden
Informations-sikkerhedsudvalget	• Udarbejde informationssikkerhedspolitikken • Udarbejde organisatorisk årshjul for informationssikkerhed. • Udarbejde plan for implementering af informationssikkerhedspolitikken, herunder ○ Igangsætte implementering (aktiviteter) for informationssikkerhedspolitikken ○ Opfølgning på implementering (styring af aktiviteter) for informationssikkerhedspolitikken (governance). • Udarbejde retningslinjer og politikker for informationssikkerhed. • Udarbejde årlig rapport på informationssikkerhed til Direktionen. •Sørger for at inddrage relevante centerchefer
Koncernledelsen	• Årlig opfølgning på informationssikkerheden i Ishøj kommune •Sikrer tilstrækkelige ressourcer •Godkender organisatoriske tiltag og aktiviteter på baggrund af oplæg fra Informationssikkerhedsudvalget
Informations-sikkerhedsteamet	•Understøtter informationssikkerhedsudvalgets arbejde •Udførende på informationssikkerhedsudvalgets opgaver •Udførende på centrale opgaver som vedrører informationssikkerheden •Rådgivning og koordinering med de lokale informationssikkerhedskoordinatorer •Rapporterer til informationssikkerhedsudvalget •Rådgivning af centerchefer/KCL
Centerchefer	•Ansvarlig for implementering af informationssikkerhedspolitikken og tilhørende aktiviteter i eget center •Ansvarlig for implementering af lokale initiativer •Ansvarlige for opfølgning på informationssikkerheden i eget center
ISK	• Koordinerer og kontrollerer lokale aktiviteter ifm. Informationssikkerhed. • Udarbejder og implementerer lokale procedurer og retningslinjer • Lokalt kontaktpunkt for centerets medarbejdere • Kontakt til Informationssikkerhedsteamet • Deltagelse i koordinatornetværket

* CISO = Chief Information Security Officer (øverste ansvarlige for informationssikkerheden i Ishøj Kommune