

INFORMATIONSSIKKERHEDSPOLITIK



SKIVEKOMMUNE

Indledning

Denne politik danner rammen for Skive Kommunes arbejde med cyber- og informationssikkerhed samt persondatabeskyttelse. Informationssikkerhedspolitikken er et fælles grundlag og en fælles forståelse af informationssikkerhed.

Det er en målsætning for Skive Kommune, at der arbejdes struktureret og klart med informationssikkerhed. Politikken skal være med til at sikre, at der er tillid til, at de data og informationer, som Skive Kommune behandler, for borgere, erhvervsliv, samarbejdspartnere og offentlige myndigheder, er tilgængelige, valide og forbliver fortrolige.

Skive Kommune skal kunne leve op til lovgivning og myndighedskrav. Samtidig er sikkerhed en del af den service, der tilbydes borgere, erhvervsliv, samarbejdspartnere og øvrige offentlige myndigheder. Politikken skal være med til at sikre, at data og informationer behandles i overensstemmelse med de krav, der stilles til kommunen, samtidig med at niveauet afbalanceres, så fleksibiliteten og dynamikken i vores dagligdag ikke mistes.

Skive Kommune er underlagt flere lovkrav, herunder NIS2-direktivet, databeskyttelsesforordningen og AI-forordningen. Kommunens regler, retningslinjer og procedurer skal være i overensstemmelse med alle sikkerhedskrav i lovgivningen og i de aftaler, der er indgået.

Skive Kommune behandler personoplysninger som led i opgaver og service. Der indsamles kun nødvendige oplysninger, og disse behandles lovligt, sikkert og fortroligt. Oplysningerne gemmes, så længe det er nødvendigt i forhold til formålet og gældende lovgivning. Adgang til oplysningerne er begrænset til relevante medarbejdere og eventuelle databehandlere. Der videregives kun oplysninger, når det er nødvendigt og lovligt. Den registrerede har altid ret til indsigt, rettelse, sletning og indsigelse mod vores behandling.

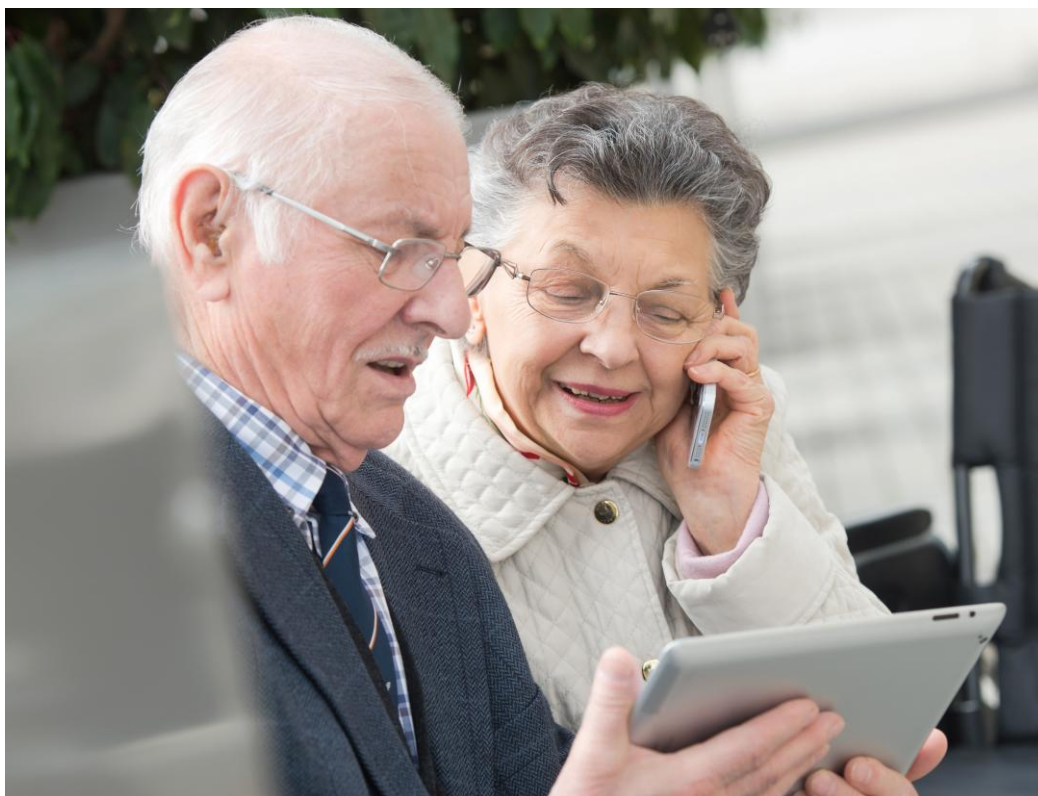
Sikkerhedsarbejdet tager afsæt i NIS2-direktivet, der har til formål at sikre et højt og ensartet cybersikkerhedsniveau på tværs af hele EU. Skive Kommune arbejder løbende med at forbedre informationssikkerheden ud fra en risikobaseret tilgang. Det betyder, at kommunen implementerer de foranstaltninger, der vurderes nødvendige for at opnå et passende sikkerhedsniveau, og at politikken samt de tilhørende retningslinjer løbende opdateres i forhold til det aktuelle trusselsbillede.



Gyldighedsområde

Ved informationssikkerhed forstår vi den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til behandling og kommunikation af data elektronisk, i papirform m.m., herunder også teknologi og organisatoriske processer. Derfor fastlægges omfanget af politikken således:

- Informationssikkerhedspolitikken gælder for alle ansatte i kommunen, uanset ansættelsesform, herunder også eksterne konsulenter og servicemedarbejdere.
- Informationssikkerhedspolitikken gælder for alle systemer og alle data, som benyttes i Skive Kommune.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til organisationens systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Skive Kommunes IT-systemer og papirarkiver.



Ledelse og styring

Byrådet har det overordnede politiske ansvar for at kommunen lever op til gældende lovgivning. Økonomiudvalget varetager den umiddelbare forvaltning og udvikling af teknologianvendelse, herunder cyber- og IT-sikkerhedsområdet.

Direktionen har det forvaltningsmæssige ansvar for Skive Kommunes informationssikkerhed. Det indebærer at træffe strategiske beslutninger om nødvendige sikkerhedsforanstaltninger og at vurdere, hvornår beskyttelse er tilstrækkelig. Direktionen har ansvaret for risikostyring, løbende kontrol og effektmåling af sikkerhedsindsatsen samt at sikre, at der er passende kvalificerede ressourcer til at arbejde med området.

Den Digitale Styregruppe udgør Skive Kommunes informationssikkerhedsudvalg og har ansvaret for, at strategiske mål oversættes og udvikles, så informationssikkerheden realiseres og efterleves. De fungerer som forandringssejere i organisationen og skal sikre at målsætninger inden for informationssikkerhed opnås.

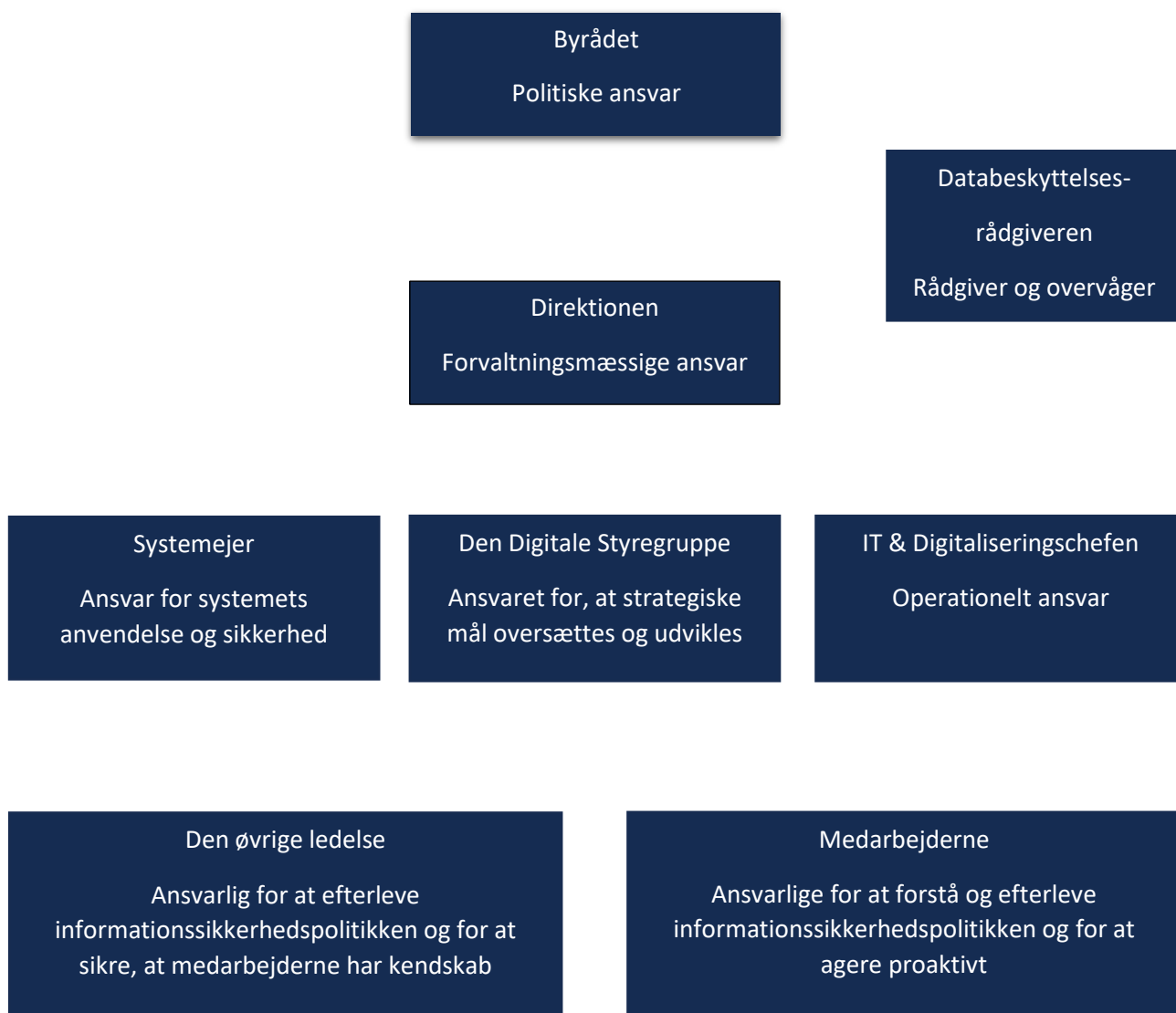
IT & Digitaliseringschefen har det operationelle ansvar for informationssikkerhedsindsatsen. Rollen omfatter formandskab for Den Digitale Styregruppe og det ledelsesmæssigt ansvar for informationssikkerhedsfunktionen. Chefen sikrer effektiv, stabil og sikker drift af kommunens IT-systemer i overensstemmelse med kommunens krav, samt at væsentlige procedurer og kontroller er tidssvarende, velbeskrevne og operationelle.

Databeskyttelsesrådgiveren rådgiver og overvåger, at kommunen behandler personoplysninger lovligt og sikkert i henhold til Databeskyttelsesforordningen. Databeskyttelsesrådgiveren rådgiver og vejleder i forbindelse med risici, udarbejdelse af politikker, databrud og beskytter borgernes rettigheder, samt fungerer som kontaktperson mellem Skive kommune, borgerne og Datatilsynet.

For alle væsentlige systemer udpeges en systemejer på chefniveau med ansvar for systemets anvendelse og sikkerhed. Systemejer identificerer sårbare dele af systemerne og tilhørende processer, sikrer efterlevelse af relevante sikkerhedsforanstaltninger og gennemfører risikovurderinger, som vurderes mindst en gang årligt.

Den øvrige ledelse er ansvarlig for at efterleve informationssikkerhedspolitikken og for at sikre, at medarbejderne har kendskab til den og overholder relevante retningslinjer i ledernes respektive områder. Medarbejderne er ansvarlige for at forstå og efterleve politikker og retningslinjer og for at agere proaktivt og bidrage til at sikre informationssikkerheden. Overtrædelser af Skive Kommunes sikkerhedsforanstaltninger kan have ansættelsesmæssige konsekvenser.

Eksterne samarbejdspartnere udfører efter kontrakt arbejde for kommunen. Den enkelte samarbejdspartner er ansvarlig for at overholde de stillede krav. Kan dette ikke lade sig gøre, skal samarbejdspartneren gøre kommunen opmærksom herpå.



Uddannelse og kompetencekrav

Ledelsen i Skive Kommune er forpligtet til at modtage løbende uddannelse i cyber- og informationssikkerhed. Uddannelsen styrker ledelsens evne til at forstå, vurdere og håndtere risici, samt at sikre et højt sikkerhedsniveau. Alle medarbejdere skal uddannes og trænes til at håndtere relevante sikkerhedsrisici, samt kende og anvende almindelige sikkerhedsvaner



Sikkerhedsforanstaltninger

Informationssikkerhedspolitikken godkendes af byrådet og direktionen. Politikken skal mindst forelægges politisk én gang pr. byrådsperiode eller ved væsentlige ændringer af enhedens forretningsmæssige mål og trusselsbillede.

Den årlige revision af informationssikkerhedspolitikken godkendes af direktionen. Direktionen modtager kvartalsvise opdateringer om status på informationssikkerheden i kommunen, fx i form af opdatering om projekter, strategiske målsætninger, handleplaner og nøgletal. På første kvartalsmøde i året fremlægges en skriftlig ledelsesrapport med status på informationssikkerheden. Denne rapport indeholder også en årlig status fra Databeskyttelsesrådgiveren.

Den Digitale Styregruppe og IT- & Digitaliseringschefen har ansvaret for, at Skive Kommune har et dækkende antal centrale retningslinjer. Retningslinjer godkendes løbende i Den Digitale Styregruppe og væsentlige retningslinjer samles til den årlige strategiske rapportering til direktionen.

Risikostyring

Databeskyttelsesforordningen bygger på en risikobaseret tilgang til informationssikkerhed. Det skal forstås sådan, at der skal foretages en kortlægning over risikoen for de registreredes rettigheder og en afvejning af risici i forhold til de forholdsregler, der bliver truffet for at beskytte de registreredes rettigheder.

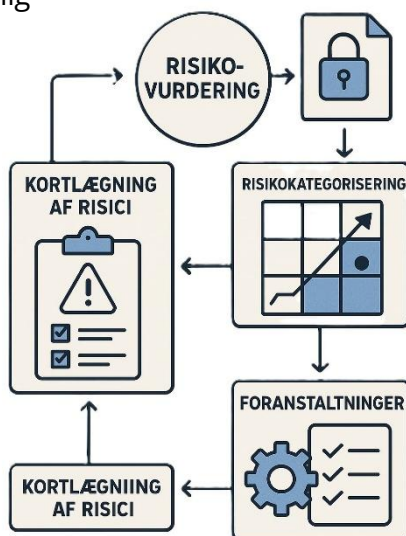
Selve risikovurderingen består af flere dele:

- En kortlægning af de risici behandlingen medfører og en kategorisering (sandsynlighed og konsekvens) heraf.
- En vurdering af hvad der er passende tekniske og organisatoriske foranstaltninger, så forordningen overholdes, og så dette kan dokumenteres.

Det er systemejerens ansvar, at der findes en risikovurdering, som ajourføres en gang årligt. Dette understøttes af IT & Digitalisering med digitaliseringskonsulenternes rejsehold. Resultaterne af en risikovurdering vil i vidt omfang kunne anvendes til at bestemme og prioritere sikkerhedsrisici og foranstaltninger. Det samlede overblik over resultatet fra risikovurderinger præsenteres årligt for Den Digitale Styregruppe og Direktionen.

Kommunens sikkerhedsniveau skal først og fremmest indfri de forventninger til troværdighed og stabilitet, der er til behandling af forretningskritiske data. Kommunen ønsker at fremstå med et sikkerhedsniveau, der tilgodeser:

- Lovgivningsmæssige krav samt EU-direktiver, inden de er omsat i national lovgivning •
- De anerkendte internationale standarder for informationssikkerhed i form af ISO 27001
- NSIS på niveau betydelig



Hændelse og beredskabsstyring

Det påhviler alle ansatte i Skive Kommune at indrapportere informationssikkerhedshændelser og svagheder i kommunens it-systemer. En informationssikkerhedshændelse kan være alt fra et tabt USB-stik til et større hackerangreb.

Skive kommune har et beredskab, der sikrer hurtig og effektiv håndtering af IT-sikkerhedshændelser og andre kritiske situationer. Det er ledelsens ansvar at sikre, at organisationen kan løse sine opgaver, når organisationen bliver udsat for ekstraordinære hændelser. Derfor skal ledere på alle niveauer, tage ansvar for beredskabsarbejdet inden for egne områder og i relevant omfang bidrage til at støtte og koordinere med andre områder og eksterne samarbejdspartnere.

IT & Digitaliseringschefen er ansvarlig for udarbejdelse og revision af IT-beredskabsplanen. Planen skal revideres i det omfang, udviklingen gør det nødvendigt. Som minimum gennemgår IT & Digitalisering beredskabsplanen én gang årligt i forbindelse med den fastlagte opfølgning på kommunens IT-sikkerhed. I tilfælde af alvorlige sikkerhedsbrud orienteres direktionen direkte fra den operative chef eller databeskyttelsesrådgiveren. Ligeledes orienteres relevante myndigheder.

Nogle informationssikkerhedshændelser vil også være brud på persondatasikkerheden (databrud) og skal indberettes til Datatilsynet. Databeskyttelsesrådgiveren overvåger, vurderer og indberetter databrud til Datatilsynet.

Version	1.1
Dokument dato	16. december 2025
Dokument forfatter	Lina Simone Bergström
Dokument ejer	Peter Molbæk
Seneste revision	-
Seneste revision godkendt af	-

Skive Kommunes byråd har godkendt informationssikkerhedspolitikken på byrådsmødet tirsdag den 16. december 2025.

Link til referat fra mødet (se punkt 28): [Byråd - Byrådssalen, Rådhuset, Torvegade 10.](#)