Plan- og Landdistriktsstyrelsen

Dato: 8 maj 2024
Version: 1
Godkendt af Informationssikkerhedsudvalget
Plan- og Landdistriktsstyrelsen

Informationssikkerhedspolitik for Plan- og Landdistriktsstyrelsen

1.1 Indledning

Plan- og Landdistriktsstyrelsens informationssikkerhedspolitik er:

1. Rammen der sætter informationssikkerhedsniveauet for styrelsen og sørger for, at denne efterleves i praksis.
2. Fastlagt ud fra den til enhver tid gældende lovgivning og best practice standarder, og følger principperne i ISO27001 standarden, persondataforordningen (GDPR) samt de tekniske minimumskrav for staten. Dette opdateres løbende i forbindelse med den gældende lovgivning.

1.2 Hovedmålsætning i informationssikkerhedspolitikken

Hovedmålet for politikken er at beskytte styrelsens informationer og systemer og at sikre styrelsen troværdighed, fortrolighed og tilgængelighed til følsomme data samt pålidelighed i datas indhold.

Politikken skal tilgodese følgende behov:

- at understøtte bevidstheden om informationssikkerhed,
- at følsomme og fortrolige informationer beskyttes og adgang kun gives ud fra et arbejdsbetinget behov,
- at informationer er pålidelige og fuldstændige,
- at anvendte it-services fungerer korrekt og sikrer stabil tilgang til data,
- at informationer og it-services er tilgængelige, når autoriserede brugere har behov for det.

Herved understøtter politikken, at Plan- og Landdistriktsstyrelsen opnår høj driftssikkerhed og minimeret risiko for nedbrud, manipulation eller tab af data.

1.3 Rolle og ansvarsfordeling

Direktionen er ansvarlig for fastlæggelsen af det overordnede strategiske niveau af arbejdet med Informationssikkerhed, herunder at informationssikkerhedsmæssige overvejelser er med i alle strategiske beslutninger.

Informationssikkerhedsudvalget er ansvarlig for det taktiske niveau af efterlevelsen af informationssikkerheden hos styrelsen, herunder udarbejdelse af awareness træning, procedurer, politikker og kontroller til at sikre efterlevelsen.

Informationssikkerhedsudvalget rapporterer minimum årligt til ledelsen på niveauet af efterlevelsen af den gældende lovgivning og standarder.

Ledelsen er ansvarlige for det operationelle niveau af informationssikkerheden, herunder at deres afdelinger kender til deres roller og ansvar og måden hvorpå, der arbejdes hos styrelsen.

Medarbejderne er selv ansvarlige for at efterleve de retningslinjer, der er udarbejdet for styrelsen samt sikre, at de arbejder korrekt i forbindelse med den træning, de har været igennem. Retningslinjerne for hvordan medarbejdere skal arbejde, er udmøntet i "Retningslinjer for Informationssikkerhed i Plan- og Landdistriktsstyrelsen", *jf. bilag 1*.

1.4 Dokumentation

Informationssikkerhedspolitikken vil udmønte sig i yderligere dokumentation, som sikrer, at alle ansatte hos Plan- og Landdistriktsstyrelsen efterlever informationssikkerheds niveauet, der er fastlagt for styrelsen. Denne yderligere dokumentation er følgende:

- Taktiske retningslinjer, *jf. bilag 1*.
- Operationelle procedurer, *jf. bl.a. bilag 2* om håndtering af hændelser.
- IT beredskabsplan, *jf. bilag 3*.

Nævnte former for dokumentation tager udgangspunkt i den fastlagte risikoappetit, risikovurdering og gældende lovgivning for styrelsen.

Chefen med ansvar for IT har i sammenspil med informationssikkerhedsudvalget ansvar for den administrative styring af arbejdet med informationssikkerhed.

Udover ovenstående dokumentation, skal der være udarbejdet beredskabsplaner til sikring af driftskontinuiteten, herunder nødplaner og genetableringsplaner for de mest forretningskritiske processer og systemer hos styrelsen. Beredskabsplanerne skal tage udgangspunkt i den gældende risikovurdering,

1.5 Risikobaseret sikkerhedsniveau

Informationssikkerhedspolitikken skal være med til at sikre, at data og informationer behandles i overensstemmelse med de krav, der stilles til organisationen. Udover gældende lovning og standarder skal procedurer, arbejdsgange og retningslinjerne være baseret på en risikovurdering, Denne risikovurdering er fundamentet for de foranstaltninger, der skal implementeres, for at sikre, at styrelsen lever op til den gældende lovgivning og standarder.

Risikovurderingen udmønter sig i en konsekvensvurdering baseret på de mest forretningskritiske processer samt en sårbarhedsvurdering baseret på de mest forretningskritiske systemer. Beslutningen om hvorvidt foranstaltninger skal gennemføres, skal afvejes i forhold til styrelsens risikoappetit samt de økonomiske og operationelle konsekvenser ved foranstaltningerne.

Plan- og Landdistriktsstyrelsen anvender ISO 27005 standarden, som retningslinje for udarbejdelsen af risikovurderingerne, som skal gennemgås årligt.

1.6 Gyldighedsområde og omfang

Politikken gælder for alle ansatte i Plan- og Landdistriktsstyrelsen, uanset ansættelsesform samt for eksterne brugere, samarbejdspartnere og leverandører. Alle medarbejdere skal derfor løbende modtage relevant uddannelse i informationssikkerhed og databeskyttelse.

Politikken omfatter alle former for informationer, der ejes, opbevares eller behandles af styrelsen og dens databehandlere. Dette gør sig gældende uanset, hvilket system, informationerne er lagret på og uanset, hvordan de fremstår.

Relevante krav til eksterne samarbejdspartnere og leverandører vedrørende informationssikkerhed skal indarbejdes og konkretiseres i aftaleforholdet, således styrelsens sikkerhedsniveau fastholdes og sikres.

1.7 Overtrædelse

Overtrædelse af styrelsens informationssikkerhedspolitik kan, efter omstændigheder, medføre sanktioner.

Alle overtrædelser skal meldes til informationssikkerhedsudvalget.

I tilfælde af situationer hvor informationssikkerhedspolitikken, af gyldige årsager ikke kan efterleves, kan der anmodes om afgivelser fra politikken. Anmodning om dispensation skal sendes til chefen med ansvar for IT og derfra vil informationssikkerhedsudvalget tage stilling til, om der kan gives dispensation. Denne vil være begrænset til en specifik målgruppe, periode samt omfang og skal godkendes af chefen for ansvar med IT og dernæst direktionen, hvis sidstnævnte skønnes nødvendigt.

1.8 Evaluering

Plan- og Landdistriktsstyrelsens informationssikkerhedspolitik revideres minimum én gang årligt. Direktionen beslutter i samråd med informationssikkerhedsudvalget, på hvilken måde informationssikkerhed og databeskyttelse skal indarbejdes i direktionens og andre relevante årsplaner, og hvordan informationssikkerhedsindsatsen konkret skal evalueres.

1.9 Offentliggørelse

Plan- og Landdistriktsstyrelsens informationssikkerhedspolitik skal formidles til alle relevante interessenter herunder samtlige medarbejdere i styrelsen og offentliggøres på insideplst.dk

1.10 Versionshistorik

Version 1.0. Godkendt af direktionen den 24. juni 2024.