Informationssikkerhedspolitik for Tønder kommune

Dokumenthistorik

SBSYS sag nummer 85.15.02-P22-1-16				
Versions-Nummer	**Dato for version**	**Godkendt af**	**Godkendt dato**	**Ansvar**
3	1.2.2023	Informationssikkerheds-udvalget	24.2.2023	Michael Holst
2	3.1.2017	Kommunalbestyrelsen	30.3.2017	Lars Møldrup
2	3.1.2017	ØK	23.3.2017	Lars Møldrup
2	3.1.2017	Direktionen	2.3.2017	Lars Møldrup
1	27.2.2014	Kommunalbestyrelsen	27.2.2014	

Seneste relevante ændringer i omvendt rækkefølge.
Fuld historik i SBSYS.

Versi-ons-Nummer	**Dato**	**Navn**	**Ændring**
3	1.2.2023	Michael Holst	Politik tilrettet med relevante organisatoriske ændringer.
2	3.1.2017	Lars Møldrup	Tilføjet afsnit om sikkerhedsniveau og brud på informationssikkerhed, samt fjernet gentagelser om ansvar

TØNDER KOMMUNE

1.1	16.12.2016	Poul Skovmand Thingholm	Ajourført politik og fjernet regler i overens-stemmelse med ISO 27001
1	27.2.2014		

TØNDER KOMMUNE

Indhold

TØNDER KOMMUNE

Indledning

Politikken beskriver Tønder Kommunes overordnede tilgang til informationssikkerhed og er udarbejdet med standarden ISO 27001 som rammen for informationssikkerhed, samt gældende lovgivning og kommunens hidtidige Informationssikkerhedspolitik.

Informationssikkerhedspolitik fastlægger formål med og rammer for IT-sikkerhed, beskriver organisering af arbejdet, samt rolle- og ansvarsfordeling.

Formål med Informationssikkerhedspolitik

Formålet med Informationssikkerhedspolitikken er at definere rammer for beskyttelse af kommunens informationer og særligt sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Derfor har ledelsen af Tønder Kommune besluttet et sikkerhedsniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler.

Sikkerhedsarbejdet tilrettelægges i overensstemmelse med anbefalingerne i informationssikkerhedsstandarden ISO27001.

Hensigten med Informationssikkerhedspolitikken er endvidere at tilkendegive over for alle, som har relation til kommunen, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer. På den måde kan IT-sikkerhedsproblemer forebygges, eventuelle skader kan begrænses og reetablering af information kan sikres.

Mål

Tønder Kommune gennemfører nødvendige aktiviteter for at sikre:

- **Tilgængelighed**
  At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud således at kommunens IT-systemer er tilgængelige for brugerne og for borgerne og virksomhederne, når de har behov for det
- **Integritet**
  At opnå en pålidelig og korrekt funktion af kommunens IT-systemer med minimeret risiko for ukorrekt datagrundlag og datatab, f.eks. som følge af menneskelige eller systemmæssige fejl, forsøg på svindel eller bedrageri samt udefrakommende hændelser
- **Fortrolighed**
  At sikre fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede og autentificerede brugere har adgang.

TØNDER KOMMUNE

Holdninger og principper

Informationssikkerhed i Tønder Kommune implementeres efter følgende overordnede principper:

- Medarbejdere skal have en bevidst holdning til begrebet IT-sikkerhed med vægt på reel sikkerhed frem for formel sikkerhed
- Informationssikkerhed skal implementeres gennem forebyggende tiltag og aktiviteter, og Tønder Kommune vedligeholder, understøtter og fastholder vidensniveauet hos alle medarbejdere for at understøtte sikker behandling af informationer i Tønder Kommunes informationssystemer
- Tønder Kommunes virke afhænger af håndteringen af informationer i elektronisk form for at leve op til de krav som borgere, samfundet og lovgivningen stiller til en effektiv administration og til en hurtig og korrekt service. Af denne grund behandles informationssikkerhed som sidestillet med forretningssikkerhed.
- Tønder Kommune arbejder med IT-sikkerhed for at underbygge Tønder Kommunes troværdighed over for omverdenen, herunder samarbejdspartnere og kommunens borgere.
- Såfremt eksterne parter berøres af sikkerhedshændelser hos Tønder Kommune, vil Tønder Kommune kommunikere ærligt og troværdigt over for berørte parter.

Rammer og gyldighed

Informationssikkerhedspolitikken gælder for alle personer, der har adgang til kommunens interne netværkstjenester eller som har adgang til informationssystemer i Tønder Kommune:

- Medarbejder i kommunen
- Politiker samt medlemmer i råd og nævn mv. i kommunen
- Samarbejdspartner, som har fået tildelt adgang.

Ansvar og organisering

IT-sikkerhedsorganisationen følger linjeorganisationen således, at ansvar og kompetencer omkring IT-sikkerhed er en integreret del af forretningsprocesserne og medarbejdernes hverdag.

Øverste IT-sikkerhedspolitikansvarlige

Kommunalbestyrelsen har det overordnede ansvar og skal godkende Informationssikkerhedspolitikken.

Direktionen er af Kommunalbestyrelsen udpeget som øverste IT-sikkerhedspolitikansvarlige og har det overordnede ansvar for, at Informationssikkerhedspolitikken til enhver tid er ajourført. Endvidere har Direktionen kompetence til at godkende IT-sikkerhedsregler samt godkende ændringer i Informationssikkerhedspolitikken.

Informationssikkerhedspolitikken med bilag vil èn gang årligt blive forelagt direktionen, hvor eventuelle ændringer gennemgås. Direktionen vurderer, hvornår der er behov for politisk behandling og evt. inddragelse af MED-systemet.

Der er almindelig delegationsret i forbindelse med IT-sikkerhedsspørgsmål.

IT-sikkerhedsansvarlig
Fagchef for Borger-, Digital- & Ejendomsservice er – med mindre andet er vedtaget – IT-sikkerhedsansvarlig.

Det daglige IT-sikkerhedsarbejde varetages af den IT-sikkerhedsansvarlige, som fungerer som øverste sikkerhedspolitikansvarliges stedfortræder i forbindelse med tilrettelæggelse af kommunens IT-sikkerhed.

I forbindelse med alvorlige brud på IT-sikkerhed refererer den IT-sikkerhedsansvarlige direkte til Direktionen.

Informationssikkerhedsudvalg
Informationssikkerhedsudvalget er placeret under Direktionen, og direktør for fagområdet digitale service er formand for udvalget.

Informationssikkerhedsudvalget består derudover af Fagchef for Borger-, Digital- & Ejendomsservice, den IT-sikkerhedsansvarlige, og af kommunens informationssikkerhedskoordinator, der fungerer som koordinator og sekretær for udvalget.

Det er informationssikkerhedsudvalgets opgave at påse, at der til stadighed er etableret forretningsgange og procedurer, som understøtter overholdelsen af Informationssikkerhedspolitikken og IT-sikkerhedsreglerne.

Informationssikkerhedsudvalget skal sikre at den overordnede Informationssikkerhedspolitik og ISO27001 standarden implementeres og efterleves i organisationen.

Ansvar hos samarbejdspartnere
Ansvaret for overholdelse af Informationssikkerhedspolitikken i forbindelse med arbejde udført af samarbejdspartnere påhviler linjeorganisationen.

Brud på informationssikkerheden
Bevidst eller ubevidst overtrædelse af sikkerhedsbestemmelserne kan medføre, at kommunens brugere, samarbejdspartnere, borgere mv. oplever kompromittering af relevante data, ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationer. Dette kan dels medføre forringelse af den kommunale service, af kommunens image, og dels et økonomisk tab.

Overtrædelse af informationssikkerhedspolitikken og hertil knyttede retningslinjer er at betragte som en tjenstlig forseelse, og skal håndteres i linjeorganisationen som sådan og i overensstemmelse med gældende personalepolitiske bestemmelser herfor.

Sikkerhedsniveau
Tønder Kommune skal træffe fornødne foranstaltninger til at beskytte oplysninger om personer mod uautoriseret anvendelse og mod fejl i de registrerede eller forarbejdede oplysninger. Sikkerhedsniveauet og IT-anvendelsen i Tønder Kommune skal til hver en tid være i overensstemmelse med gældende lovgivning og skal sikre, at kommunen kan opfylde sine kontraktuelle forpligtelser.

Tønder Kommune fastlægger på baggrund af konkret risikovurdering et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer. Tønder Kommune gennemfører en balanceret risiko- og konsekvensvurdering.

TØNDER KOMMUNE

I al behandling af data sikrer Tønder Kommune korrekt sikkerhed og beskyttelse af data, samt at data er valide:

- Alle data har en entydig autoritativ kilde dvs. data fødes og vedligeholdes hvor viden om data er, og når data benyttes uden for den autoritative kilde, skal disse altid være opdaterede og retvisende i forhold til den autoritative kilde
- Medarbejdere sikres adgang til alle nødvendige data for at træffe oplyste og korrekte beslutninger i en given sag i henhold til gældende lovgivning
- Den korrekte identitet bag en given adgang til systemerne er kendt og autoriseret.

Opfølgning og kontrol

Tønder Kommune måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Løbende entydig registrering og opfølgning på hændelser inden for informationssikkerhedsområdet
- Løbende registrering af alle tiltag inden for informationssikkerhedsområdet
- Opfølgning på vidensniveau inden for informationssikkerhedsområdet i Tønder Kommune

For at sikre en levende og ajourført Informationssikkerhedspolitik skal følgende elementer underkastes en årlig gennemgang:

- Informationssikkerhedspolitikken
- IT-sikkerhedsregler og -procedurer
- Risikoanalyser og -vurderinger
- Systemejer-lister.

Beredskabsplanlægning

I samarbejde med leverandører af kommunens IT-drift, skal der etableres et beredskab, som skal sikre, at Tønder Kommune i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske forretningsmæssige aktiviteter inden for en ledelsesgodkendt tidshorisont. Større driftsnedbrud eller katastrofer betyder tab af tilgængelighed af væsentlige systemer, udstyr og/eller faciliteter, hvorfor reetablering af tilgængeligheden af disse er et centralt område i beredskabsplanlægningen.

Der skal minimum én gang årligt foretages en gennemgang af den aktuelle beredskabsplan.

Godkendt

Denne politik er vedtaget af Tønder Kommunes kommunalbestyrelse den 30. marts 2017.