NORDDJURS KOMMUNES INFORMATIONSSIKKERHEDSSTRATEGI
STRATEGI – ORGANISERING – ANSVAR

Indholdsfortegnelse

1. Indledning

Norddjurs Kommune er en del af en verden, som hele tiden forandrer sig – hvad end det er på lokalt, nationalt eller internationalt plan. Der kommer konstant nye teknologier, mere digitalisering af samfundet samt nye aftaler og lovgivning, som vi skal tage stilling til. De mange forandringer sætter bæredygtighed i fokus, for at skabe en verden, hvor vi fortsat kan levere en høj kvalitet af service til alle Norddjurs Kommunes borgere. Norddjurs Kommune er en aktiv deltager i arbejdet med FN's 17 verdensmål for en bæredygtig udvikling, og det ønsker vi også at understøtte igennem vores arbejde med data. Både de arbejdsgange vi har nu, og dem vi måtte udvikle på sigt.

Arbejdet med bæredygtighed, giver derfor Norddjurs Kommune anledning til at arbejde med en ordentlig og bæredygtig databehandlingskultur. Vi skal passe godt på vores og borgernes værdifulde informationer, så vi kan nå i mål med de fokusområder i FN's 17 verdensmål, som Norddjurs Kommune har udvalgt at arbejde med til dagligt.

Vi forstår en bæredygtig databehandlingskultur som, en struktureret og gennemsigtig tilgang til at behandle data i en verden med stigende datamængder og digitaliserede arbejdsgange. Hvor sociale fordele[1] ved en behandling afvejes med sikkerhedsmæssige risici og økonomiske gevinster eller tab. Hvor vi inddrager vores interessenter under hele databehandlingsprocessen, og i åbenhed vurderer de risici der kan være forbundet med en behandling, for sammen at finde den bedste løsning.

Det er vigtigt at vores omverden har tillid til hvordan vi behandler data, uanset om vi arbejder med personoplysninger eller andre forretningsinformationer. Dataene skal være fortrolige, når det er nødvendigt. De skal fremstå korrekte, og ikke kunne manipuleres eller ændres uhensigtsmæssigt, så vi træffer beslutninger på et informeret grundlag. Dataene skal også være tilgængelige, til de autoriserede ansatte, når der er et behov for dem. Målet for den gode informationssikkerhed er derfor, at vi kan opnå vores hovedmålsætninger, uden at data kompromitteres i under vejs.

Dette afføder, at vi arbejder struktureret med informationssikkerheden. Strategien for informationssikkerhed er en overordnet plan, som kaster lys på de delmål vi skal arbejde med, og desuden giver et struktureret overblik over rollerne og ansvaret i informationssikkerhedsarbejdet.

Informationssikkerhed er ikke målet i sig selv, men skal ses som et vigtigt element af kommunens virksomhed, som understøtter, at vi når i mål med vores andre politikker, strategier og kerneopgaver, og fortsat har fokus på borgernes rettigheder. Disse kunne konkret være vores Plan- og udviklingsstrategi, Digitaliseringsstrategi eller Velfærdsteknologipolitikken.

[1] Sociale fordele skal forstås som de fordele digitalisering og øgede datamængder skaber i samfundet.

2. Norddjurs Kommunes strategi for informationssikkerhed

Norddjurs Kommunes informationssikkerhedspolitik oplister en række målsætninger, som organisationen løbende skal arbejde med, så kommunen altid opnår tidssvarende sikkerhed. Denne strategi skal være med til at operationalisere målsætningerne, så de bliver opnåelige og målbare. Desuden beskriver strategien også i detaljeret grad hvordan arbejdet i organisationen er organiseret i henhold til roller og ansvar (se kapitel 3).

Kommunen har mange interessenter, som bliver påvirket af niveauet af informationssikkerhed. Det kan fx være borgere, lokale foreninger, personalet eller politikerne. Men der findes også mange interessenter, som ikke påvirkes direkte af informationssikkerhedsniveauet, men stadig har en stor indflydelse på hvordan kommunen indretter sikkerheden. Disse interessenter kan fx være leverandører, tilsynsmyndigheder eller nationale og internationale lovgivere.

Det er vigtigt at strategien afspejler, hvorvidt interessenterne påvirkes af informationssikkerhed, og om disse har indflydelse på kommunens sikkerhedsniveau.

Illustration 1 viser et samlet billede af kommunens interessenter for informationssikkerhed.

Illustration 1: Norddjurs Kommunes interessenter i informationssikkerheds arbejdet

2.1 Hvad skal sættes i fokus?

Vores interessenter forventer, at Norddjurs Kommune behandler oplysninger fortroligt, når dette er påkrævet, at oplysningerne altid er korrekte, så vi træffer de rigtige afgørelser og at vores autoriserede personale kan tilgå oplysningerne når det er nødvendigt. Desuden er der klare forventninger om, at kommunen overholder gældende lov og aftaler.

For at organisationen kan sikre fortroligheden, integriteten og tilgængeligheden af data, er det vigtigt at både personale og ledelse har de nødvendige kompetencer, og at de systemer vi anvender har et tilstrækkeligt sikkerhedsniveau og efterlever lovgivning og aftaler. Desuden skal det være muligt at finde tilstrækkelige retningslinjer og procedurer for arbejdsgange, så der ikke er tvivl om for hverken ledelse eller personale, hvordan behandling af data eller IT-aktiver skal forekomme.

Norddjurs Kommune er derfor afhængig af at udvælge leverandører som understøtter kommunens informationssikkerhedspolitik. Herudover, er kommunen afhængig af et kendskab til nationale og internationale tilsynsmyndigheders og lovgiveres krav til beskyttelsen af data, samt holde sig informeret om, hvordan den bredere offentlige forvaltning i Danmark forholder sig til lovgivning og aftaler.

Kommunen skal ligeledes fokusere på, at dokumentation af retningslinjer og procedurer for arbejdsgange bliver udformet, for at ledelse og personale kan træffe beslutninger på et informeret grundlag. Dokumentationen skal også tage højde for kommunens tværfaglighed og mangfoldige kerneopgaver. Retningslinjer og procedurer må derfor ikke udformes på en sådan måde, at forvaltningen ikke kan udføre sin myndighedsudøvelse eller forvaltningsvirksomhed.

Det efterstræbes, at det konkrete sikkerhedsniveau vurderes ud fra et afbalanceret forhold mellem sociale fordele, forretningsmæssige informationsrisici, risici for de registreredes rettigheder og kommunens økonomiske forhold.

Sikkerhedsniveauet skal afspejle de trusler og sårbarheder der findes for Norddjurs Kommune, dog går gældende lovgivning og persondatarettighederne forud for kommunens ressourcemæssige forhold.

2.2 Afgrænsning af strategien

Informationssikkerhed har en bred snitflade både i organisationen og for eksterne interessenter. Derfor skal alle som udgangspunkt være bekendte med politikken, relevante tværgående retningslinjer for informationssikkerhed og deres rolle og ansvar i organisationen.

Ledelsen og nøglemedarbejdere, inden for informationssikkerhed, fx informationssikkerhedskoordinatoren og IT-sikkerhedsgruppen, har et større ansvar for at sikre et tilstrækkeligt sikkerhedsniveau.

Roller og ansvar beskrives i kapitel 3.

2.3 Målsætninger

Målsætningerne for Norddjurs Kommunes informationssikkerheds- og databeskyttelsesarbejde skal være operationaliserede i sådan grad, at de kan udføres med et taktisk spillerum. Det er dog vigtigt, at det nemt kan vurderes, hvorvidt organisationen har opnået det den ville i informationssikkerhedspolitikken.

Målene tager udgangspunkt i Norddjurs Kommunes nuværende kontekst. Det vil sige opstartsfasen, for kommunens strukturering af informationssikkerhedsarbejdet. Nogle af opgaverne, der er listet som delmål, vil allerede være under udarbejdelse eller i drift, men strategien lægger op til, at disse mindst revideres, så de forbliver tidssvarende.

De konkrete delmål er opdelt på de overordnede målsætninger, som kommunalbestyrelsen har godkendt d. 25. august 2020. Målsætningerne skal revideres i forlængelse af en evt. revidering af kommunens overordnede informationssikkerhedspolitik, eller når delmålene i strategien er opnået. Hensigten er, at målene i tabel 1, skal opnås i løbet af kommunalbestyrelsesperioden 2021-2025.

Tabel 1: Målsætninger for awarenessarbejdet i Norddjurs Kommune fordelt på overordnede emner.

Skabe opmærksomhed og udvikle kompetencerne om informationssikkerhed og databeskyttelse i hele kommunen
• Der udarbejdes en separat strategi for informationssikkerhed og databeskyttelsesawareness.
Styre kommunens arbejde med sikkerheden gennem en risikobaseret styringsmetode
• En central risikometode udvælges til at sikre risikostyring i Norddjurs Kommune. • Alle fagområder, sekretariater og staben skal opliste, vurdere og kategorisere deres informationsaktiver. • Informationsaktiver der er vurderet vigtige for den kommunale virksomhed eller de registreredes rettigheder skal risikovurderes. • Risici der overskrider organisationens risikovillighed skal håndteres enten ved at acceptere, flytte, stoppe eller formindske risikoen. Håndteringen skal dokumenteres. • Informationsaktiver der vurderes meget kritiske for organisationen eller de registreredes rettigheder, skal have udarbejdet en beredskabsplan. • Nye behandlinger af personoplysninger skal risikovurderes inden behandlingen påbegyndes. • Norddjurs Kommunes samlede risikobillede skal afrapporteres årligt til direktionen.
Sikre fortrolighed af kommunens informationer, således kun autoriserede kan tilgå oplysningerne
• Ud fra en risikobaseret styringsmetode, skal de kritiske systemer udvælges og have dokumenteret adgangsstyrings processerne for det pågældende system, herunder både digitale og fysiske systemer. • Der skal opsættes struktur omkring autorisationskontrol, som baserer sig på risikovurderinger af de pågældende autorisationer der kontrolleres. • Kommunen skal inddeles i dokumenterede sikkerhedszoner, hvoraf fremgår hvilket sikkerhedsniveau er påkrævet for adgang til zonen. • Der skal føres fysiske tilsyn af kommunens fagområder, staben og sekretariaterne for håndtering af fysiske dokumenter. • Der skal beskrives generelle procedurer for, hvordan dokumenter med fortrolige oplysninger bortskaffes. • Der skal beskrives retningslinjer for, hvordan afdelingerne håndterer fortrolige oplysninger generelt, herunder fra at oplysningerne indgår i kommunen til de arkiveres eller slettes. • Der skal etableres en beredskabsplan for større lækager af fortrolige oplysninger, herunder muligheder for kommunikation og begrænsning af skader • IT-afdelingen skal supplere med en strategi for sikring af kommunens oplysninger på digitale enheder, samt tekniske foranstaltninger som anti-virus, firewall, patching, netværkssegmentering, kryptering, data discovery m.m.
Sikre integritet af kommunens informationer, så de fremstår korrekte og ikke uhensigtsmæssigt ændres eller manipuleres
• Etablere procedurer der løbende sikrer datakvaliteten af indgående oplysninger til kommunen. • Etablere logning i systemer der behandler personoplysninger. • Etablere en struktur der sikrer, at kun de nødvendige brugere har privilegerede rettigheder. • Der skal være etableret en backup af kritiske systemer, og der skal foretages en årlig test af backuppen. • Der skal være etableret retningslinjer for adgangsstyring, som sikrer imod uautoriseret ændring af oplysninger. • Der skal være etableret slette- og arkiveringsprocedurer for personoplysninger. • Ud fra en risikobaseret styringsmetode, skal de kritiske systemer udvælges, og have etableret foranstaltninger, som sikrer dataintegriteten imod destruktion eller tab.
Sikre tilgængelighed til kommunens informationer, så autoriserede kan tilgå de oplysninger der kræves, for at kommunens services kan udføres

- Der skal etableres en central plan for leverandørstyring, som sikrer at kommunen kan tilgå tilkøbte platforme når det er nødvendigt, og desuden sætter kriterier for systemernes generelle niveau af sikkerhed. Herunder skal der også tages stilling til kommunens exit-strategi.
- Ud fra en risikobaseret styringsmetode, skal de mest kritiske systemer i kommunen have udformet beredskabsplaner ift. nødløsninger.
- Beredskabsplanerne skal testes mindst en gang årligt som skrivebordstest, og hvert tredje år som fuld test.

Sikre, at kommunen udviser ansvarlighed ved dokumentation af overholdelse af relevante aftaler og lovgivning

- Dokumentation for hvordan kommunen overholder og forholder sig til databeskyttelseslovgivningen skal udformes.
- Der skal vedtages tværgående retningslinjer for informationssikkerheden i Norddjurs Kommune.
- Retningslinjer og procedurer skal udformes, hvor det er vurderet relevant ud fra en risikobaseret styringsmetode, for brugen af digitale og fysiske systemer.
- Det skal faciliteres, at kommunens databeskyttelsesrådgiver uvildigt kan føre tilsyn med, at kommunen overholder databeskyttelseslovgivningen.
- Skabe overblik og procedure for vedligeholdelse af kommunens IT-kontrakter, herunder også databehandleraftaler.
- Strukturere og udføre tilsyn hos kommunens databehandlere ud fra en risikobaseret styringsmetode.

Sikre, at informationssikkerheden ikke nedprioriteres i kommunen på usagligt grundlag

- Der skal etableres processer for jævnlig afrapportering til kommunens informationssikkerhedsudvalg, direktion og kommunalbestyrelse, herunder med fokus på kommunens sikkerhedshændelser og risikobillede.
- Kommunen skal indgå i tværgående netværk på nationalt plan, for at sikre indflydelse og kongruens med andre offentlige myndigheder.
- Ressourcetildeling til området skal basere sig på en årlig evaluering af kommunens informationssikkerhedsniveau, dertil også databeskyttelsesrådgiverens årsrapport.

2.4 Ansvarlige for målopfyldelse

De ansvarlige for målopfyldesen i Norddjurs Kommune er primært direktionen, systemejerne, informationssikkerhedsudvalget, databeskyttelsesrådgiveren og IT-sikkerhedsgruppen. Men alle ansatte har et medansvar for, at kommunens databehandlingskultur er bæredygtig.

Informationssikkerhedskoordinatoren rapporterer kvartalsvis til informationssikkerhedsudvalget vedr. status af arbejdet med målopfyldelse, herunder revidering af politikker og retningslinjer, sikkerhedshændelser i kommunen og kommunens risikobillede. Informationssikkerhedsudvalgets formand rapporterer som udgangspunkt en gang årligt om status til kommunens direktion.

IT-sikkerhedsgruppen og informationssikkerhedskoordinatoren skal løbende sikre, at IT-sikkerhedsniveauet er tilstrækkeligt. IT-sikkerhedsgruppen rapporterer enten til koordinatoren eller informationssikkerhedsudvalget om status. Denne status skal ligeledes indgå i den årlige afrapportering til kommunens direktion.

Informationssikkerhedsudvalget og systemejerne har ansvaret for, at der findes de tilstrækkelige retningslinjer og procedurer i kommunen. Udvalget beskæftiger sig med tværgående retningslinjer og procedurer i kommunen, hvor systemejerne fokuserer på lokale systemer og arbejdsgange.

Der skal foretages årligt tilsyn af kommunens efterlevelse af databeskyttelseslovgivningen af databeskyttelsesrådgiveren. Tilsynet skal, efter databeskyttelsesrådgiverens egen bestemmelse og vurdering, udmøntes i databeskyttelsesrådgiverens statusrapport. Rapporteringen skal ske til kommunalbestyrelsen og direktionen.

Se kapitel 3 og 4 for en uddybende beskrivelse af organisering og ansvar.

2.5: Opfølgning og løbende evaluering

Opfølgningen og den løbende evaluering skal være en simpel målopfyldelsesevaluering, med en tilknyttet analyse af resultaterne. Resultaterne af første løbende evaluering skal afrapporteres i første kvartal af 2022 af informationssikkerhedskoordinatoren til informationssikkerhedsudvalget og direktionen.

Den endelige evaluering skal ske inden næste kommunalbestyrelsesperiodes udløb (2021-2025).

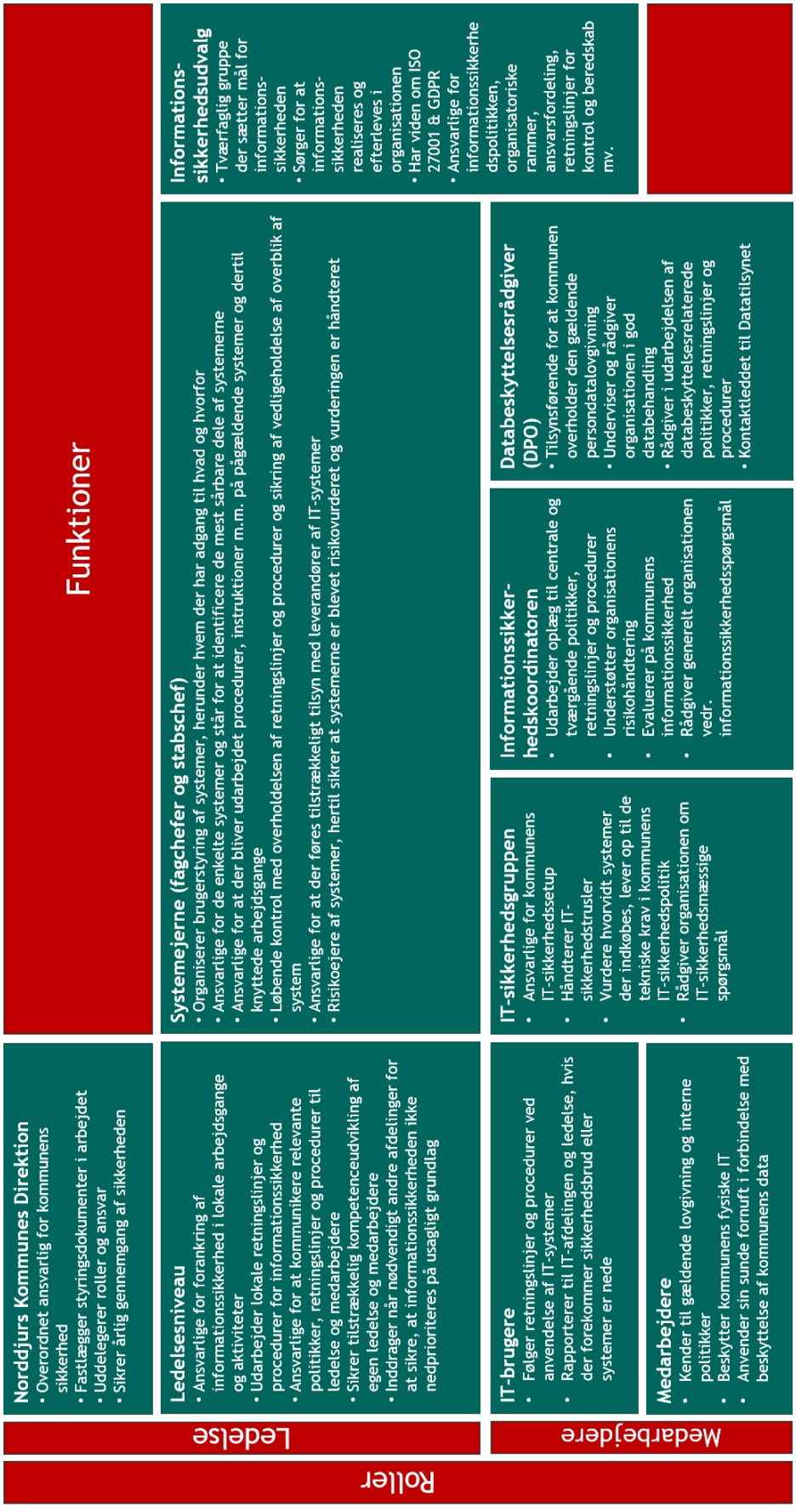
3. Organisering og ansvar i informationssikkerhedsarbejdet

I kapitel 3 beskrives Norddjurs Kommunes organisering af informationssikkerhedsarbejdet. Dette er helt fra direktionens roller og ansvar til kommunens frontlinjemedarbejdere. Det er vigtigt at huske på, at uanset hvilken rolle man har i sit almindelige virke, vil der være en snitflade til informationssikkerheden i kommunen. Enten i form af, at man som direktion sætter en retning for sikkerhedsarbejdet, som IT-specialist implementerer sikkerhedstiltag på computere, IT-systemer og netværk, eller som medarbejder blot sikrer, at fortrolige dokumenter er låst inde.

På næste side findes model 2, som viser et generelt overblik over kommunens organisering i informationssikkerhedsarbejdet. Derefter kommer der uddybende beskrivelser for diverse roller, og hvilke opgaver disse roller løfter i arbejdet.

Beskrivelserne er målrettet ledelsen, som skal kende organiseringen i informationssikkerhedsarbejdet. Det forventes ikke at medarbejdere kender denne struktur til fulde, men at de i stedet ved hvad deres eget ansvarsområde er. Derfor kan beskrivelserne også anvendes ved nyansættelser af medarbejdere, for at klarlægge hvad de ansatte skal være opmærksomme på, når de arbejder i Norddjurs Kommune.

Model 2: Overblik over organiseringen af informationssikkerhedsarbejdet.



3.1: Direktionen

Direktionen består af kommunaldirektøren samt fagdirektørerne, og er overordnet ansvarlig for kommunens informationssikkerhed, herunder databeskyttelse.

Kommunens strategi og politik for informationssikkerhed fastlægges af direktionen. Direktørerne er ansvarlige for den ledelsesmæssige forankring af arbejdet, herunder prioritering og kommunikation ud til kommunens ledelse og medarbejdere. Desuden skal direktionen sikre et tilstrækkeligt niveau af ressourcer i arbejdet.

3.1.1: Direktionens opgaver

Direktionen er overordnet ansvarlig for kommunens informationssikkerhed og databeskyttelse, og hertil hører bl.a. flg. opgaver:

- Indstille kommunens overordnede informationssikkerhedspolitik til kommunalbestyrelsen
- Fastlæggelse af strategi for informationssikkerhed og databeskyttelse
- Uddelegere roller og ansvar i arbejdet, herunder forankring af ansvaret i ledelsen
- Fastlæggelse af kommunens risikovillighedsniveau
- Sikre tilstrækkelige ressourcer inden for arbejdet, herunder økonomiske og organisatoriske konsekvenser
- Kommunikere strategier, politikker, roller og ansvar ud i organisationen
- Årlig gennemgang af status for arbejdet, herunder forholde sig til kommunens risikobillede og -villighed
- Forholde sig til sager vedr. informationssikkerhed og databeskyttelse, der kan have større konsekvenser for kommunen eller de registrerede

3.1.2: Hvem bistår direktionen

For at lykkes med arbejdet, kræver det opbakning og bistand fra organisationen. Overordnet set er hele Norddjurs Kommune ansvarlig for at sikre et højt niveau af informationssikkerhed, men i praksis supporteres direktionen af informationssikkerhedsudvalget, informationssikkerhedskoordinatoren og databeskyttelsesrådgiveren.

Hertil kan bl.a. nævnes flg. opgaver som disse aktører skal bistå direktionen med:

- Informationssikkerhedsudvalget bistår i den daglige ledelse og drift af tiltag inden for informationssikkerhed og databeskyttelse
- Informationssikkerhedskoordinatoren bistår til den årlige afrapportering inden for IS
- Databeskyttelsesrådgiveren bistår både med vejledning inden for databeskyttelse samt en årlig afrapportering inden for databeskyttelse

3.2: Informationssikkerhedsudvalget

3.2.1: Hvad er informationssikkerhedsudvalget

Informationssikkerhedsudvalget er nedsat af direktionen, og er det styrende organ inden for informationssikkerhed og databeskyttelsesarbejdet til der til dagligt koordinerer, at tiltag inden for arbejdet realiseres og efterleves i organisationen.

Udvalget består af 10 medlemmer, hvoraf 8 er faste medlemmer, og 2 medlemmer er udpegede repræsentanter for kommunens forvaltninger. Chefgrupperne i de respektive forvaltninger udpeger deres repræsentant.

Faste medlemmer:

- Chefen for Borgerservice, IT og Digitalisering (Formand)
- Lederen af IT (teknisk sikkerhed)
- Lederen af Digitalisering (organisatorisk implementering)
- Informationssikkerhedskoordinatoren
- Databeskyttelsesrådgiveren
- Stabschefen
- Sekretariatschefen for Velfærdsforvaltningen
- Sekretariatschefen for Fællesforvaltningen

3.2.2: Informationssikkerhedsudvalgets opgaver

Informationssikkerhedsudvalget koordinerer kommunens arbejde for informationssikkerhed og databeskyttelse, herunder at kommunens niveau af informationssikkerhed er tilfredsstillende. Udvalgets hovedopgaver består af flg.:

- Vedligeholde gældende informationssikkerhedspolitik og retningslinjer, samt godkende nye.
- Forholde sig til Norddjurs Kommunes problematikker og nuværende risici angående informationssikkerhed, herunder også persondatabeskyttelse.
- Rådgive og indstille til direktionen om nye tiltag vedrørende informationssikkerhed.
- Koordinerer at de vedtagne tiltag kommunikeres ud i organisationen.
- Igangsætte awarenesstiltag i organisationen, for at sikre tilstrækkelig bevågenhed om informationssikkerhed, herunder også persondatabeskyttelse.
- Behandle problematikker angående informationssikkerhed, herunder også persondatabeskyttelse, der kræver skærpet bevågenhed, og indstille emner til behandling i direktionen.
- Bistå at informationssikkerhedsarbejdet kan lykkes i Norddjurs Kommune.

For at lykkes med ovenstående opgaver, kræver det desuden, at udvalget bistås af informationssikkerhedskoordinatoren, IT-sikkerhedsgruppen, systemejerne såvel som kommunens støttestrukturer.

3.3: Informationssikkerhedskoordinatoren

3.3.1: Hvem er informationssikkerhedskoordinatoren

Informationssikkerhedskoordinatoren arbejder til dagligt med forankring af informationssikkerhedstiltag i organisationen, og bistår udvalget og direktionen med oplæg om nye tiltag. Udover udvalget og direktionen, er koordinatoren også den som støtter mellemledelsen og medarbejdere i informationssikkerhedssager.

Tiltag er fx oplæg til nye politikker der vedrører informationssikkerhed i kommunen, risikometode til udarbejdelse af risikovurderinger eller er med til at uddanne personale om informationssikkerhed.

Herudover har koordinatoren ansvar for, at sikkerhedshændelser og -brud registreres til central evaluering, så det kan vurderes hvorvidt mere eller mindre sikkerhed er behøvet.

Koordinatoren har et tæt samarbejde med IT-sikkerhedsgruppen, for at disse organer kan sparre omkring den tekniske sikkerhed i kommunens IT-systemer.

3.3.2: Informationssikkerhedskoordinatorens opgaver

Koordinatoren har ansvaret for generel udarbejdelse, implementering, forankring og evaluering af diverse informationssikkerhedstiltag. Dette munder sig konkret ud i flg. opgavetyper:

- Udarbejde oplæg til informationssikkerhedspolitikken og relaterede politikker
- Understøtte organisationens risikohåndtering, herunder med udarbejdelse af en risikometodik og generel understøttelse af kommunens risikovurderingsarbejde

- Udarbejder i samarbejde med lokale afdelinger retningslinjer og generelle dokumenter vedr. informationssikkerhedsarbejdet.
- Registrere, følge op på og evaluere sikkerhedshændelser og -brud i kommunen
- Rådgive organisationen vedr. informationssikkerhedssager
- Undervise og igangsætte opmærksomhedskampagner for personale om informationssikkerhed
- Understøtte informationssikkerhedsudvalgets arbejde, herunder med udarbejdelse og opsætning af mødebilag
- Generelt evaluere informationssikkerhedsniveauet i kommunen
- Aflægge årlig rapport om informationssikkerheden i kommunen til informationssikkerhedsudvalget

3.4: IT-sikkerhedsgruppen

3.4.1: Hvem er IT-sikkerhedsgruppen

IT-sikkerhedsgruppen består af afdelingslederen for IT-afdelingen og udvalgte medarbejdere i IT-afdelingen, der har fokus på den tekniske sikkerhed i kommunens IT-systemer som del af deres daglige arbejde. Gruppens medlemmer udpeges af lederen af It-afdelingen, med afsæt i medarbejdernes kompetence inden for IT-sikkerhed.

Arbejdet består fx af opsætning af firewalls eller antivirus-systemer, sikring imod uautoriserede adgang til kommunens netværk, sikring af det fysiske driftsmiljø og håndtering af potentielle cyberangreb rettet imod organisationen.

Desuden har IT-sikkerhedsgruppen kompetence til at rådgive organisationen om IT-sikkerhedsmæssige spørgsmål.

3.4.2: IT-sikkerhedsgruppens opgaver

IT-sikkerhedsgruppen har det praktiske ansvar for, at kommunens IT-systemer er optimalt beskyttede imod organisatoriske, udefrakommende og miljømæssige trusler. Dette munder konkret ud i flg. typer af opgaver:

- Holde sig opdateret med udviklingen inden for IT-sikkerhed og cybertrusler, herunder best-practice for beskyttelsen af IT-aktiver
- Benchmarking af kommunens IT-sikkerhedsniveau
- Indstilling af nye IT-sikkerhedstiltag i organisationen
- Opsætning og drift af IT-sikkerhedsmæssige tiltag for systemer, netværk og hardware
- Understøtte risikovurderinger af IT-systemer ud fra et IT-sikkerhedsmæssigt perspektiv
- Vurdere hvorvidt systemer der indkøbes, lever op til kommunens IT-sikkerhedspolitik
- Håndtering af IT-sikkerhedstrusler, fx cyberangreb, oversvømmelse af serverrum eller nedbrud
- Bistå organisationen under IT-revision
- Sikre overholdelse og ajourføring af de IT-tekniske aspekter af beredskabsplanerne, som IT-afdelingen har ansvaret for
- Jævnlig dialog med informationssikkerhedskoordinatoren vedrørende IT-sikkerhedsmæssige sager
- Rådgive organisationen omkring IT-sikkerhedsmæssige spørgsmål

IT-sikkerhedsgruppen er en essentiel og understøttende del af kommunens informationssikkerhedsorganisering, som er med til at sikre, at IT-driften af kommunens kerneopgaver, ikke forstyrres af diverse former for trusler.

3.5: Systemejerne (chefer)

3.5.1: Hvem er systemejer

Chefer i Norddjurs Kommune er ansvarlige for et eller flere administrative- eller fagområder. Hvis området har tilknyttet et IT-system, så er chefen tilsvarende ansvarlig for IT-systemet. Det gør chefen til systemejer.

Fx er chefen for arbejdsmarkedsområdet ansvarlig for dette fagområde. Arbejdsmarkedsområdet har tilknyttet Schultz Fasit som it-system. Det gør arbejdsmarkedschefen til systemejer for it-systemet Schultz Fasit.

Systemejeren er således den øverst ansvarlige for et eller flere IT-systemer med de muligheder og forpligtelser der følger med ejerskabet.

Hovedprincippet ved placering af systemejerskab er:

- Ejerskab placeres ved den chef, der har ansvaret for området og de forretningsprocesser, som det pågældende IT-system understøtter.

Hvis hovedprincippet ikke er dækkende, så placeres ejerskabet ud fra følgende underprincipper:

- Ejerskabet placeres hos den chef, der beslutter anskaffelse og livscyklus for IT-systemet.
- Ejerskabet placeres hos den chef, der har den største brugerflade.
- Ejerskabet placeres hos den chef, der er ansvarlig for budget til IT-systemet.

Ved større organisationsændringer revurderes placering af systemejerskab.

3.5.2: Hvad betyder det at være systemejer

Systemejeren er overordnet ansvarlig for IT-systemet, men får hjælp fra IT, Digitalisering, Indkøb, Økonomi, m.fl. til at løfte ansvaret. Systemejer beslutter organisering i og omkring IT-systemet, herunder bl.a.:

- Organisering af superbrugere og slutbrugere
- Arbejdsgangstilrettelæggelse inkl. de arbejdsgange der knytter it-systemer sammen i flows
- Systemanvendelse ift. gældende lov, fx forvaltningslov, offentlighedslov, arkivlov, persondatalov, fagområdets lov, m.v.
- Sikrer udarbejdelse af relevante retningslinjer og procedurer for IT-systemer og arbejdsgange
- Budgetopfølgning og budgetoverholdelse
- Årlig kontrol af system- og kontraktoverblikket for systemejerens pågældende systemer
- Løbende kontrol med relevante leverandører, herunder databehandlere

Systemejeren er desuden dataejer og risikoejer. Dvs. at systemejer er ansvarlig for kvaliteten af data der anvendes i systemet, og ansvarlig for risiciene der findes ifm. anvendelsen af systemet.

Systemejeren kan uddelegere opgaver i tilknytning til ovenstående.

Indkøb af nye IT-systemer, fornyelse af kontrakter på eksisterende IT-systemer og tilkøb af moduler og services til IT-systemer sker i et samarbejde mellem systemejer, IT og Indkøb. Behandles personoplysninger i systemet, skal databeskyttelsesrådgiveren ligeledes inddrages.

Kontraktovervågning med særlig opmærksomhed på kontraktudløb og leverandørkontrol af kontrakter foregår i OS2 KITOS, der er Norddjurs Kommunes Contract Management system.

Basis-IT der er grundplatform for effektiv anvendelse af det pågældende IT-system sikres af IT og Digitalisering.

Teknisk implementering af IT-systemer foregår primært i IT med relevant inddragelse af fagområdet for at sikre det tekniske setup matcher det organisatoriske behov.

Den organisatoriske adgang- og rettighedsstyring foregår i de enkelte fagområder. Den tekniske tildeling foretages af Norddjurs Kommunes Helpdesk, på baggrund af instruktioner fra de ansvarlige.

Overholdelse af persondataforordning sker hos systemejer på baggrund af rådgivning fra databeskyttelsesrådgiveren, herunder risikovurdering, trusler og sikkerhedsforanstaltninger. Dokumentation for overholdelse af databeskyttelsesforordningen samles bl.a. i OS2 Kitos.

3.6: IT-brugere

3.6.1: Hvem er IT-brugere

IT-brugere er både ansatte i kommunen, eksterne konsulenter eller samarbejdspartnere med adgang til et eller flere af IT-systemer. Autorisationens adgang og fratagelse til IT-systemer gives af systemejerne og autorisationsansvarlige.

Fx er man IT-bruger, hvis man har adgang til kommunens Outlook, eller har adgang til KMD Nexus, OPUS el. lignende systemer.

En IT-bruger er derfor en ansat, konsulent eller samarbejdspartner, som har fået autoriseret adgang til vilkårlige IT-systemer, i forbindelse med deres arbejdsopgaver.

3.6.2: Hvad betyder det at være IT-bruger

IT-Brugere i et eller flere af kommunens IT-systemer, har et personligt ansvar i at overholde de fastsatte retningslinjer og procedurer for anvendelsen af IT-systemer.

Fx har en bruger fået tildelt nogle bestemte rettigheder i et IT-system, hvor brugeren har mulighed for at se andre ansattes løn. I nogle tilfælde, er brugeren berettiget til at tilgå disse oplysninger i forbindelse med en arbejdsopgave. Adgang til oplysninger uden et arbejdsrelateret grundlag, vil anses som misbrug af brugerens beføjelser.

IT-Brugere har derfor flg. ansvarsopgaver i informationssikkerhedsarbejdet:

- Følge retningslinjer og procedurer for arbejdet i IT-systemer
- Beskytte deres brugerlogin og passwordoplysninger
- Etiske og moralske forpligtelser til de IT-systemer brugeren har adgang til
- Rapportere til IT-afdelingen, hvis IT-systemer er nede
- Rapportere til nærmeste leder/chef, hvis der dages, at uautoriserede ansatte/udefra kommende har adgang til IT-systemerne
- Gå til nærmeste leder/chef, hvis de finder uregelmæssigheder i IT-systemer

3.7: Medarbejdere (alle)

3.7.1: Hvad betyder det at være medarbejder

For at nå i mål med Norddjurs Kommunes målsætninger for informationssikkerhed, kræves det, at alle medarbejdere tager medansvar for sikkerheden. Medarbejdere sikrer, at de uddelegerede opgaver udføres på en måde, hvorpå kommunen efterlever både lovgivning og interne politikker.

Medarbejderne bør derfor være opmærksomme på, hvilke retningslinjer der gælder for deres område. Hvis ikke dette er tydeligt, er det også medarbejderens ansvar at udpege det overfor egen ledelse.

Medarbejdere kommer i kontakt med forskellige former for data, information og fysisk sikkerhed i deres arbejdsgang, og derfor skal medarbejderne være bekendt med informationssikkerhedspolitikken og de gældende retningslinjer for ønsket adfærd på området.

Medarbejdernes ansvar indebærer herunder:

- Generel overholdelse af gældende lovgivning og interne politikker
- Udpege mangler i gældende politikker og retningslinjer
- Beskytte kommunens fysiske IT, fx ved at låse ubrugte computere og mobiler inde
- Informere om potentielle risici og konkrete hændelser til nærmeste leder, IT-afdelingen eller databeskyttelsesrådgiver

- Anvende sin sunde fornuft, når det gælder beskyttelse af kommunen og borgernes informationer

Medarbejderes rolle i kommunens informationssikkerhedsarbejde er vigtig, da medarbejderne i høj grad på et eller andet tidspunkt i deres arbejdsgang, kommer i kontakt med enten fysiske eller digitale data, som skal være fortrolige, korrekte eller tilgængelige.

Medarbejdernes rolle i at påpege mangler og trusler samt forhindre disse, er derfor essentielt i at sikre et højt informationssikkerhedsniveau i Norddjurs Kommune.

4. Støttestrukturer i informationssikkerhedsarbejdet

Dette kapitel beskriver kommunens støttestrukturer i arbejdet med informationssikkerhed. Det vil sige, at enhederne der er beskrevet, skal understøtte kommunen med at sikre et tilstrækkeligt niveau af informationssikkerhed og databeskyttelse. Støttestrukturerne skal derfor heller ikke forstås som alene ansvarlige for, at lovgivning overholdes eller at sikkerheden er tilstrækkelig i fagområderne.

4.1: Databeskyttelsesrådgiveren

4.1.1: Hvad er en databeskyttelsesrådgiver

Databeskyttelsesrådgiveren, også kendt som DPO'en[2], er en rådgivende og kontrollerende funktion. DPO'en skal inddrages i sager omhandlende databeskyttelse, og være med til at bistå kommunens efterlevelse af databeskyttelsesforordningen, også kendt som GDPR[3]. Rådgiveren hjælper derudover de registrerede[4], hvis de henvender sig vedr. persondataretlige sager.

4.1.2: Hvad er databeskyttelsesrådgiverens rolle og opgaver

DPO'en er kontaktleddet til Datatilsynet og varetager en række opgaver i forbindelse med dette. Den primære opgave i Norddjurs Kommune, er at føre kontrol, underrette, undervise, skabe opmærksomhed og rådgive kommunen om implementering og overholdelse af lovgivning og interne politikker ift. beskyttelse af personoplysninger. Flg. opgaver bl.a. dem rådgiveren arbejder med:

- Rådgive kommunens ansatte og borgere omkring persondataretten og databeskyttelse
- Tilsyn af kommunens overholdelses af GDPR
- Rådgivning i forbindelse med udarbejdelse af risikovurderinger og konsekvensanalyser
- Anmelde sikkerhedsbrud til Datatilsynet
- Kontaktpersonen for Datatilsynet angående spørgsmål og behandling af personoplysninger.
- Databeskyttelsesrådgiveren skal indgå og støtte informationssikkerhedsudvalget gennem input ift. politikker vedr. persondata.
- Undervise og skabe opmærksomhed omkring databeskyttelse i kommunen
- Rådgive om udvikling og vedligeholdelse af intern dokumentation om beskyttelse af personoplysninger

Rådgiveren bistår hele organisationen i spørgsmål relateret til databeskyttelse, men er ikke ansvarlig for kommunens efterlevelse af GDPR. Alle i kommunen har generelt et ansvar for, at loven bliver overholdt på lige fod med forvaltningsloven, offentlighedsloven, osv.

[2] DPO står for Data Protection Officer, som er den engelske betegnelse for databeskyttelsesrådgiver.
[3] GDPR står for General Data Protection Regulation, som er den engelske betegnelse for databeskyttelsesforordningen.
[4] De registrerede er personer, som kommunen behandler personoplysninger om. Borgere, ansatte, m.m.