UDKAST

NORDDJURS KOMMUNES RISIKOMETODE

Godkendt af Norddjurs Kommunes direktion d. XX.XX.XXXX

Indholdsfortegnelse

1. Indledning 3
2. Formål 3
3. Anvendelsesområde 3
4. Ansvarlige for risici 3
5. Databeskyttelsesforordningen og ISO 27001 4
6. Processen for risikostyring 4
6.1: Etablering af kontekst 4
6.2: Risikovurdering 4
6.3: Risikohåndtering 4
6.4: Risikoaccept 5
7. Norddjurs Kommunes kontekst og forretningsprocesser 6
8. Risikovurderinger 8
8.1: Konsekvensanalyse 10
9. Risikohåndtering 11
9.1: Acceptere risici 11
9.2: Flytte risici 11
9.3: Undgå risici 11
9.4: Mindske risici 11
10. Opfølgning 12
11. Afrapportering til øverste ledelse 12
Bilag 1 – Procedure for risikostyring 13
Bilag 2 – Eksempler på afdelingernes informationsaktiver 14
Bilag 3 – Trusselsoversigt 17
Bilag 4 – Eksempler på risici for den registrerede 20

1. Indledning

Sikkerhed, omkring vores informationer og systemer, har aldrig været vigtigere, end i dag. Kriminalitet, cybertrusler, tekniske og menneskelige fejl, klimaforandringer eller ulykker i det omkringliggende miljø er alle årsager til, at vores informationer kan blive kompromitterede.

Vi kan miste adgang til kritiske informationer, informationerne kan blive beskadiget, ændret, slettet eller manipuleret og vi kan risikere, at fortrolige oplysninger bliver lækket og offentliggjort. Den potentielle skade, kan betyde større økonomiske konsekvenser, tab af tillid fra omverdenen og i værste tilfælde dødsfald.

Derfor skal vi tage stilling til vores sikkerhed af informationer, og hvor det er muligt, forebygge hændelser, så informationerne ikke kompromitteres.

Til dette formål, skal vi først kende vores informationer, hvilke risici de kan udsættes for, sandsynligheden af risiciene og hvilke konsekvenser der medfølger. En risiko kunne fx være at sende fortrolige oplysninger til en forkert modtager. Hvor sandsynlig er hændelsen, og hvad er konsekvenserne? Når vi kender resultatet, kan vi vurdere, hvorvidt flere sikkerhedstiltag bør foretages. Det er risikostyring i en nøddeskal. Vi styrer vores sikkerhed, efter de risici der findes i kommunen.

Kerneværdien for vurderingen i risikostyring er *sund fornuft*. Risikostyring skal ikke anskues som en videnskab. Vi skal altid tage højde for, at vi udfører bestemte services, hvor en ydelse kan trumfe sikkerheden, vice versa. Det vigtigste at huske er, at vi baserer vores valg på en saglig vurdering, og dokumenterer hvorfor vi træffer en bestemt beslutning.

2. Formål

Dette dokuments hovedformål er at give Norddjurs Kommune en fælles dokumenteret tilgang til risikostyring. Dokumentet forsøger ydermere at belyse følgende delformål:

- Introducere risikostyring til ledelse og relevante medarbejdere
- Beskrive anvendelsesområde og ansvarlige for risikostyring
- Beskrive lov- og standardkrav for risikostyring
- Bidrage med eksempler på processen
- Beskrive, hvordan Norddjurs Kommune omsætter risikostyring i praksis

3. Anvendelsesområde

Risikostyringsmetodikken der er beskrevet heri, er gældende for alle Norddjurs Kommunes afdelingers informationer, hvad end de findes i fysiske lokationer eller IT-aktiver. Foruden informationer, anvendes metodikken desuden på kommunens IT-systemer.

Metoden skal følges som beskrevet, for at opnå en harmonisering i hele kommunen.

4. Ansvarlige for risici

Norddjurs Kommunes direktion er ansvarlig for at tilvejebringe en model for risikovillighed der kan anvendes i hele organisationen. Kommunens risikobillede[1] bliver løbende koordineret i Informationssikkerhedsudvalget og Direktionen får mindst én gang årligt en status på dette risikobillede. Risikobillede og risikovillighed er beskrevet i afsnit 8 og opfølgning afdækkes i afsnit 10.

Kommunens systemejere på de faglige områder (chefniveauet) er ansvarlig for risici og udførsel af risikovurderinger på de pågældende fysiske og digitale systemer, som de er ejere af, herunder informationerne systemerne indeholder. Risici på IT-systemer sker i tæt samarbejde med IT og Digitalisering. Den ansvarlige for en risiko betegnes også som 'risikoejer'. Risikoejeren skal håndtere risici på organisationens vegne. Håndtering af risici afdækkes i afsnit 9.

5. Databeskyttelsesforordning og ISO 27001

Der er to hovedårsager til, at Norddjurs Kommune skal foretage risikostyring af informationer. Kravene stammer fra databeskyttelsesforordningen, som trådte i kraft i Den Europæiske Union d. 25. maj 2018, og den fællesoffentlige digitaliseringsstrategi 2016-2020, vedtaget af Regeringen Lars Løkke Rasmussen III, Kommunernes Landsforening og Danske Regioner i maj 2016.

Forordningen stiller krav til, at behandlingssikkerhed foretages ud fra en vurdering af risici for de

[1] Risikobilledet er de trusler, sårbarheder og risici kommunen står med på nuværende tidspunkt.

registreredes rettigheder og frihedsrettigheder. Hvis der findes en høj risiko ved behandling af personoplysninger, skal den med andre ord sikres yderligere eller ikke foretages.

Digitaliseringsstrategien pålægger kommunerne at følge ISO 27001-kravstandardens principper, for at højne informationssikkerhedsniveauet blandt offentlige myndigheder. Grundelementet i standarden er, at der foretages risikostyring i organisationen. Heraf skal der udarbejdes risikovurderinger af forretningsinformationer, hvad end disse informationer består af.

Det er derfor vigtigt, at Norddjurs Kommune laver risikostyring, og har en skærpet opmærksomhed på informationer som er personoplysninger.

6. Processen for risikostyring

Processen for risikostyring kan opdeles i 4. stadier (se model 1 s. 5.) Stadierne er *etablering af kontekst*, *risikovurdering*, *risikohåndtering* og *risikoaccept*. Denne proces skal gennemføres årligt og ved større organisatoriske forandringer eller hvis nye trusler opstår, hvilket påkræver en revurdering af risikobilledet.

6.1: Etablering af kontekst

Første stadie for risikostyring er, at vi kender den kontekst vi befinder os i. Norddjurs Kommune er en unik organisation, som behandler en lang række informationer dagligt, og som står overfor helt bestemte typer af trusler. Vi skal derfor have kendskab til vores forretningsgang, informationerne der indgår heri, og de trusler der findes, som kunne have konsekvenser for kommunen. Dette kunne eksempelvis være ondsindede personer, der vil stjæle informationer eller holde information som gidsel (ransomware), indtil en løsesum betales. Fysiske elementer kan også være en trussel, fx en å der går over sine breder og oversvømmer kommunens faciliteter.

Start derfor ud med at kende den kontekst, som skal vurderes. Hvad omhandler processen, og hvilke oplysningerne indgår i den? Hvis processen startede op, hvilke trusler ville der så være knyttet til den?

Eksempel

Distancearbejde er blevet en mere almindelig arbejdsform. Ved distancearbejde skelnes der som udgangspunkt ikke om, hvilke informationer en medarbejder kan arbejde med. Altså er fortrolige oplysninger ikke begrænset til arbejdspladsen.

Distancearbejde skaber nye trusler. Tab af informationer, fx ved glemsel eller mistet under transport. Der kan være større sandsynlighed for informationslæk, fx hvis medarbejderen ikke har et fortroligt rum at tale i på distancen, eller hvis medarbejderen ikke har en korrekt måde at afskaffe fortrolige dokumenter.

6.2: Risikovurdering

Når der er dannet et overblik over informationsaktiver, behandlinger og trusler, skal der foretages en vurdering af sandsynligheden og konsekvensen ved indtræden af de pågældende trusler, for henholdsvis kommunen og den registrerede.

Konkret gøres dette ved at vurdere både sandsynligheden og konsekvensen på en skala fra 1-4, og gange de to tal sammen. Hvis det endelige tal overstiger kommunens risikovillighed, skal der foretages yderligere risikohåndtering. Hvis tallet er lig med, eller tæt på risikovilligheden, skal vi desuden tage stilling til, om vi kan implementere nemme og omkostningsfrie foranstaltninger, for at reducere risikoen yderligere.

6.3: Risikohåndtering

Efter en risikovurdering skal risikoejeren tage stilling til de risici, som overstiger kommunens risikovillighed. Risikoejeren har 4 muligheder for risikohåndtering:

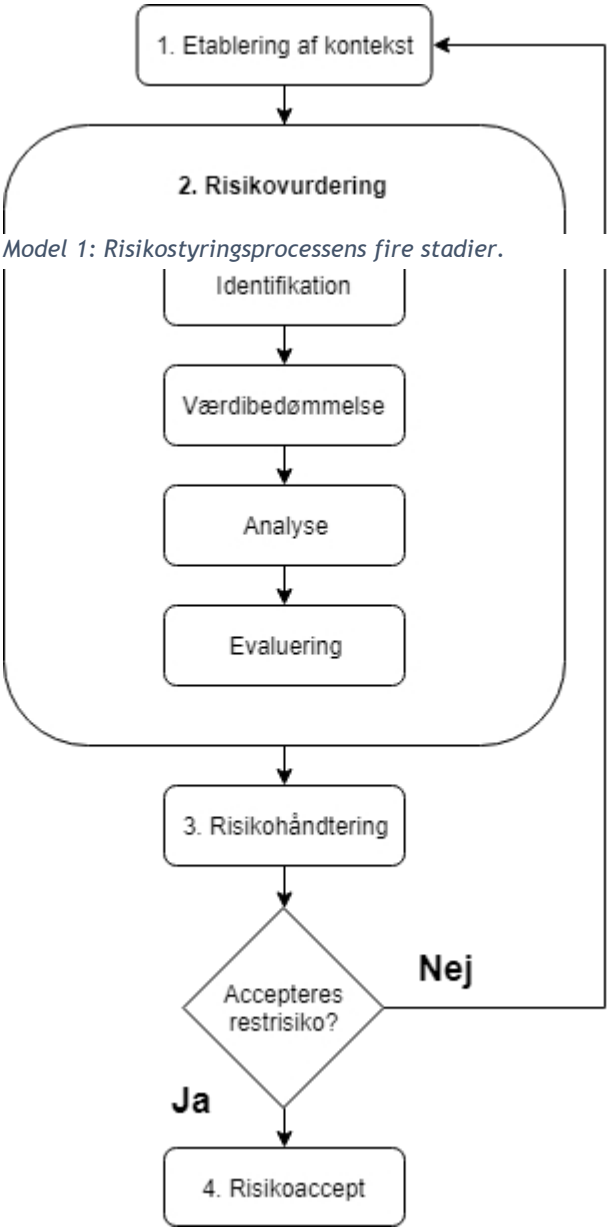
1. Acceptér risikoen - Der foretages ikke yderligere.
2. Flyt risikoen - Risikoen flyttes til en tredjepart, fx en forsikring eller outsourcing.
3. Undgå risikoen - Aktiviteten der leder til risikoen stoppes eller ændres.
4. Kontrollér – Risikoen mindskes ved at indføre nye sikkerhedstiltag, som reducerer enten sandsynlighed eller konsekvens for risikoen.

Håndteringen skal dokumenteres, og eventuelle opgaver der knytter sig til håndteringen skal uddelegeres.

6.4: Risikoaccept

Fjerde og sidste stadie er en accept af risikoen. Der vil som udgangspunkt altid være en risiko for en given hændelse, hvad end den er minimal eller

relativt høj. Det er risikoejerens ansvar, at denne 'restrisiko' accepteres.



Model 1: Risikostyringsprocessens fire stadier.

7. Norddjurs Kommunes kontekst og forretningsprocesser

Norddjurs Kommune har en bred kontekst, da kommunen udbyder mange forskellige services og håndterer forskellige typer infrastruktur. Det giver derfor bedst mening at tage udgangspunkt i kommunens enkelte forretningsområder, som hver afdeling håndterer, fx Skole- og Dagtilbuds-

området, Vej og Ejendom eller Staben. Hver afdeling har et kerneområde, hvor de benytter informationer til unikke behandlinger.

Når der etableres en kontekst, er det derfor ideelt at tænke over, hvilke informationsaktiver og behandlinger af personoplysninger afdelingen foretaget. Se bilag 1 for eksempler på informationsaktiver i afdelingerne, tag evt. også udgangspunkt i afdelingens KLE-numre og faglove.

Hernæst skal I opliste de trusler som jeres afdeling kan stå overfor. Fx ondsindede medarbejdere eller borgere, hackere eller fysiske trusler som oversvømmelse. Se bilag 2 for en overordnet trusselsoversigt, der også lister frekvensen af de pågældende trusler for Norddjurs Kommune som helhed. Vurderingen er foretaget centralt i Norddjurs Kommune, og den kan derfor variere.

Når listen af aktiver og behandlinger er færdig, vurderes konsekvensen af manglende fortrolighed, integritet og tilgængelighed for de pågældende aktiver og behandlinger. Dette gøres ud fra kommunens perspektiv ift. informationsaktiver og behandlingen af personoplysninger ud fra de registreredes perspektiv. Kommunens perspektiv er fx indvirkning på forretningsgangen eller driften af arbejdet, den registreredes perspektiv omhandler, hvilke konsekvenser et fortrolighedsbrud fx har for deres rettigheder eller frihedsrettigheder.

Hjælpeboks 1: Eksempler på informationsaktiver og behandlinger af personoplysninger

Et eksempel i Sundhed- og omsorgsområdet, kunne være journaler, der indeholder personoplysninger.

Et eksempel i Skole- og dagtilbudsområdet, kunne være håndskrevne noter, der blev taget til et møde.

Et eksempel i Borgerservice, IT og digitalisering, kunne være systemet, som styrer nummer i borgerservice, der påviser hvilken borger, der skal betjenes.

Hjælpeboks 2: Eksempler på trusler

Trusler som kunne ramme en afdeling, kunne eksempelvis være:

- Hackerangreb (ransomware)
- Tekniske fejl i udstyr
- Ødelæggelse af udstyr pga. brand
- Informationer sendes til forkerte modtager pga. menneskelig fejl
- Uærlige medarbejder misbruger rettigheder
- Fysiske dokumenter lækkes, fordi de står ulåst
- Strømsvigt

Konsekvensskalaer for virksomheden og den registrerede
1 vurderes lav værdi - 4 vurderes høj værdi.

Konsekvensskala for virksomheden	Konsekvensskala for de registrerede
1. Ubetydelig (uvæsentlig) Ingen særlig påvirkning for virksomhedens drift eller omdømme	**1. Offentlig viden** Informationen er offentlig tilgængelig, og tab heraf har ingen indvirkning på de registreredes rettigheder
2. Mindre alvorlig (generende) Meromkostninger, ekstra ressourceforbrug, mindre forringelse af omdømme, forringet forhold til samarbejdspartnere, forbigåelse af regler og procedurer	**2. Ikke fortroligt eller følsomt** Informationen er af almindelig karakter, og har kun i begrænset omfang indvirkning på de registreredes rettigheder, hvad end de lækkes, ændres eller ikke er tilgængelige
3. Meget alvorlig (kritisk) Der vil ske store tab af økonomi, omdømme eller troværdighed, væsentligt ressourceforbrug, lovbrud, personskade, uretmæssig videregivelse af almindelige personoplysninger	**3. Fortroligt el. overvejende fortroligt, men ikke følsomt** Kompromitterede oplysninger har betydelig konsekvens for de registreredes rettigheder, hvis de lækkes, ændres eller ikke er tilgængelige
4. Graverende (uacceptabelt) Ledelsen må aftræde, menneskeliv på spil, kommunen kan underlægges administration, essentielt samarbejde bryder sammen, kritisk lovgivning overtrædes, enkeltes rettigheder krænkes	**4. Følsomt** Kompromitterede informationer har stor konsekvens for de registreredes rettigheder, hvis de lækkes, ændres eller ikke er tilgængelige, fx med døden til følge eller diskrimination

Tabel 1: Informationsværdikategorisering

8. Risikovurderinger

En risikovurdering tager udgangspunkt i den etablerede kontekst. Når vi har lavet en liste, over de informationer vi anvender, og vurderet konsekvensen af, at behandlingen eller aktivet mister fortrolighed, integritet eller tilgængelighed, ved vi også, hvorvidt vi skal foretage en risikovurdering. Det er god praksis at vurdere alle behandlinger af personoplysninger, men det er vigtigst at fokusere på de områder, hvor konsekvensen er højest ved kompromitterede data.

Listen over informationer og trusler giver et overblik, som vi nu skal identificere risikoscenarier ud fra. Det vil sige, at man overvejer hvilke risikoscenarier som kan forekomme, hvis man fx udbetaler kontanthjælp, placerer en server i kælderen eller arbejder på distancen. Hvad kan der ske ved disse behandlinger, som får fortrolighed, integritet eller tilgængelighed til at gå tabt?

Dernæst vurderes det hvor sandsynligt det er, at en hændelse indtræffer. Vurderingen skal baseres på egne historiske data, oplysninger fra andre kommuner, statslige myndigheder (fx Center for Cybersikkerhed) eller nyhedsmedierne. Husk også at indtænke de nuværende sikkerhedsforanstaltninger, som kommunen allerede har implementeret, når sandsynligheden beregnes. Sandsynligheden skal ligesom konsekvensen vurderes på en 1 – 4 skala.

Hjælpeboks 2: Forklaring af begreberne 'fortrolighed', 'integritet' og 'tilgængelighed'.

Fortrolighed	**Integritet**	**Tilgængelighed**
Kun autoriserede brugere har adgang til informationerne.	Informationerne kan ikke blive utilsigtet ændret eller manipuleret.	Informationerne er tilgængelige for de autoriserede brugere.

Hjælpeboks 3: Eksempler på risikoscenarier.

Et eksempel på et risikoscenarie kunne være i Skole- og dagtilbudsområdet, hvor IT-systemet Aula bryder ned, hvilket medfører mistet tilgængelighed til skoleskemaer, vikardækning og lokalebookninger.

Et andet eksempel på et risikoscenarie kunne være i Borgerservice, IT og Digitalisering, hvor en ansat ved en fejl sendte følsomme personoplysninger til en forkert modtager, hvilket er et brud på fortroligheden.

Et tredje eksempel på et risikoscenarie kunne være i Sundhed- og omsorgsområdet, hvor forkerte oplysninger i en patientjournal, fx medicinoplysninger, ville være et brud på integritet.

Tabel 2: Sandsynlighedsskala

Sandsynlighed
1. Usandsynligt Hændelsen vil næppe forekomme
2. Mindre sandsynligt Det kan ske, at hændelsen forekommer
3. Sandsynligt Det forventes at hændelsen vil forekomme
4. Meget sandsynligt Hændelsen vil uden tvivl forekomme

Bemærk! I skal indtænke de nuværende sikkerhedsforanstaltninger, når I vurderer sandsynlighed og konsekvens.

Tallet fra sandsynlighed og konsekvens ganges derefter med hinanden. Her får vi en risikoscore, som skal sidestilles med kommunens risikovillighed. Er risikoscoren højere end risikovilligheden, skal der tages stilling til nye sikkerhedsforanstaltninger.

Hjælpeboks 4: Beregning af risikoscore

Sandsynlighed × Konsekvens = Risikoscore
Eksempel: Mindre sandsynligt(2) × Meget alvorlig(3) = Risikoscore(6)

Se tabel 3 for en visualisering af risikobilledet.

Tabel 3: Risikobilledet med eksempel fra hjælpeboks 4.

Sandsynlighed				
4	(4): 0	(8): 0	(12): 0	(16): 0
3	(3): 0	(6): 0	(9): 0	(12): 0
2	(2): 0	(4): 0	(6): 0	(8): 0
1	(1): 0	(2): 0	(3): 0	(4): 0
Konsekvens	1	2	3	4

En risiko i det grønne felt betyder, at Norddjurs Kommune accepterer restrisikoen uden videre. En risiko i det gule felt betyder, at Norddjurs Kommune kan acceptere restrisikoen, men kan overveje at mindske risikoen, hvis det er muligt med nye sikkerhedsforanstaltninger. Er risikoen i det røde felt, så indikerer scoren eller målingen, at kommunens risikovillighedsgrænse er overskredet. Når risikoscoren er i det røde felt, så skal der etableres nye sikkerhedsforanstaltninger for enten at begrænse sandsynligheden for en hændelse eller konsekvensen af hændelsen. Grænsen for risikovillighed er den fastlagte og dermed accepteret grænse for hele organisationen.

Risikovilligheden** i Norddjurs Kommune er **6

Risikovilligheden er sat til 6, da det indfanger hændelser med både en høj sandsynlighed og/eller en høj konsekvens. Det kan være konsekvenser med både ressource- og/eller omdømmemæssige konsekvenser for Norddjurs Kommune.

I arbejdet med modellen i praksis er det vigtig at overveje om en risikoscore i det gule felt har tendens til at stige eller falde. F.eks. kan en stigning i sandsynlighed hurtigt få scoren til at flytte fra gul til rød, da mange risikoscenarier mhp. konsekvensen typisk placeret højt for den registrerede.

Der er i denne model med bl.a. risikovillighed indhentet inspiration fra andre organisationer, herunder f.eks. Datatilsynet.

Hvis der foretages nye sikkerhedsforanstaltninger der f.eks. flytter en risikoscore fra rød til gul, så skal disse tiltag dokumenteres som en del af den dokumenterede risikostyring.

Bemærk, det er risikoejeren, der i sidste ende accepterer en risiko på vegne af organisationen.

8.1: Konsekvensanalyse

Norddjurs Kommune skal foretage en konsekvensanalyse ved persondatabehandlinger, som sandsynligvis medfører en høj risiko for de registreredes rettigheder. Den skal *kun* foretages, hvis man ud fra en risikovurdering at fundet, at det ikke er muligt at reducere risiciene til et acceptabelt niveau med nye foranstaltninger.

Konsekvensanalysen skal foretages før den pågældende behandling starter.

Formålet med en konsekvensanalyse er at vurdere, om man kan implementere den rette sikkerhed i behandlingen. Hvis analysen viser, at dette ikke er muligt at mindske risikoen, skal Datatilsynet give tilladelse til behandlingen eller den skal stoppes.

Konsekvensanalysen skal indeholde en systematisk beskrivelse af behandlingsaktiviteterne, hertil retsgrundlaget for behandlingen. En konkret vurdering af, om behandlingsaktiviteterne er nødvendige, og står i rimeligt forhold til formålet med behandlingen. En vurdering af risiciene for de registreredes frihedsrettigheder ift. behandlingen. En gennemgang af de sikkerhedsforanstaltninger, som påtænkes, kan mindske risiciene i behandlingen.

Kommunen kan være fritaget at foretage en konsekvensanalyse, såfremt der foreligger en national analyse af behandlingerne, fx i forbindelse med en lovvedtagelse. Der findes ingen konkrete eksempler på dette pt.

I forbindelse med udarbejdelse af en konsekvensanalyse, skal databeskyttelsesrådgiveren inddrages til at bistå og rådføre om opgaven.

9. Risikohåndtering

Der er 4 muligheder for risikohåndtering. Disse er at acceptere, flytte, undgå eller mindske en risiko. Det er vigtigt at risikohåndteringen dokumenteres. Denne dokumentation skal ske i skabelonen 'Ledelsesresume af risikovurdering af X'. Se bilag 1 for en konkret beskrivelse af Norddjurs Kommunes procedure for risikostyring.

9.1: Acceptere risici

Hvis Norddjurs Kommune uden videre kan acceptere en risiko, uden at etablere nye sikkerhedsforanstaltninger. Dette betyder også, at kommunen ikke foretager sig yderligere efter risikovurderingen.

9.2: Flytte risici

Kommunen kan vælge at flytte sin risiko til tredje part, fx en leverandør eller en forsikring. Ved at flytte risikoen er kommunen stadig overordnet ansvarlig, men tredje part bliver ansvarlig for håndtering af risikoen. Med andre ord, flytter kommunen en risiko enten ved indkøb af en leverandørs ydelser eller forsikrer sig imod den.

Notér dertil, at forsikringer kun gælder ud fra et kommunalperspektiv. Vi kan ikke forsikre os imod tab af registreredes rettigheder!

9.3: Undgå risici

Kommunen kan desuden vælge at undgå en risiko. Ved undgåelse forstås, at man ikke vælger at udføre en bestemt behandling, fordi man ikke kan mindske risikoen tilstrækkeligt. En risiko kan fx have for store konsekvenser, uden der findes plausible løsninger der kan mindske sandsynligheden eller konsekvensen, eller løsningen der skal mindske dem kan være for dyr at implementere.

Der kan være behandlinger med høj risiko, som vi ikke kan undgå, som del af kommunens service.

9.4: Mindske risici

Kan kommunen ikke acceptere eller flytte en risiko, og ønskes behandlingen ikke stoppet, skal der iværksættes nye sikkerhedsforanstaltninger. Nye sikkerhedsforanstaltninger kan fx være en lås på døre, nye procedurer for ansatte, opmærksomhedskampagner eller nye IT-sikkerhedstiltag.

Vælges denne mulighed for risikohåndtering, skal de nye foranstaltninger tilføjes i risikovurderingen, således man udregner den nye risikoscore. Er risikoen under kommunens risikovillighed, kan den accepteres uden videre. Hvis risikoen stadig er for høj, må det atter overvejes hvorvidt risikoen skal flyttes, undgås eller mindskes igen.

10. Opfølgning

Risikovurderinger skal med jævne mellemrum revideres, fordi risici kan ændre sig. Derfor skal der laves opfølgning mindst én gang årligt, eller ved større organisatoriske omstruktureringer.

Trusselsbilledet som Norddjurs Kommune står overfor, kan også ændre sig, hvis der fx opstår nye cybertrusler eller miljøet omkring kommunens faciliteter ændres mere eller mindre markant.

Afdelingerne anbefales derfor at iværksætte procedurer, der sikrer en årlig revidering af deres risikovurderinger. Revidering kan forekomme én gang årligt eller løbende gennem året.

11. Afrapportering til øverste ledelse

Opfølgning på risikostyring opsamles i Informationssikkerhedsudvalget og afrapporteres til Direktionen. Det samlede risikobillede indgår endvidere som et tema i forbindelse med databeskyttelsesrådgiverens årlige rapport til Økonomiudvalg og Kommunalbestyrelse.

Informationssikkerhedsudvalget aftaler i løbet af modellens første leveår, hvordan afrapportering konkret skal foregå. Det vil ske i takt med, at Informationssikkerhedsudvalget får bedre kendskab til arbejde med risikovurderinger og med afsæt i denne risikometode.

Bilag 1 – Procedure for risikostyring

Denne procedure er skrevet ud fra en forventning om, at læseren har stiftet bekendtskab med risikostyringsmetoden og dens begreber.

Proceduren beskriver, hvordan Norddjurs Kommune i praksis udarbejder risikovurderinger.

Skabeloner

Følgende skabeloner skal anvendes:

- Skabelon til risikovurderinger (excel)
- Skabelon til ledelsesresume af risikovurdering af X (word-dokument)

Arbejdsgang

Ved opstart af en ny behandling af personoplysninger, indkøb eller anvendelse af nye informationsaktiver (fx indkøb af nye typer af computere), eller ved involvering af en IT-leverandør eller ekstern konsulent, skal der foretages en risikovurdering.

Risikovurderingen skal indgå som en del af processen for Norddjurs Kommunes projektarbejde.

Det er essentielt, at risikovurderingen er foretaget, hvis en IT-leverandør eller ekstern konsulent påbegynder at behandle *personoplysninger*, på vegne af Norddjurs Kommune.

Følg de nedenstående skridt ved udformning af en risikovurdering:

1. Anvend 'Skabelon til risikovurderinger' og følg vejledningen i excel-arket
2. Efter risikovurderingen i excel-arket er færdig, anvend 'Skabelon til ledelsesresume af risikovurdering af X'. Følg instruktionerne i skabelonen
3. Gem dokumentet med en korrekt og sigende titel "Ledelsesresume af risikovurdering af X behandling"
4. Opsummer risikobilledets uacceptable risici i ledelsesresumeet
5. Beskriv anbefalinger til nye sikkerhedsforanstaltninger, som kan reducere de identificere risici til et acceptabelt niveau
6. Udfyld tabellen for risikoejerens risikohåndtering
7. Afgiv ledelsesresume samt excel-ark til den pågældende leder
8. Send en kopi af ledelsesresume og excel-ark til kommunens informationssikkerhedskoordinator
9. Journaliser de pågældende dokumenter

Journaliseringen skal følge journaliseringsprincipperne. Det vil sige, at risikovurderingen skal journaliseres på det rette systems eller den rette ydelses samlesag.

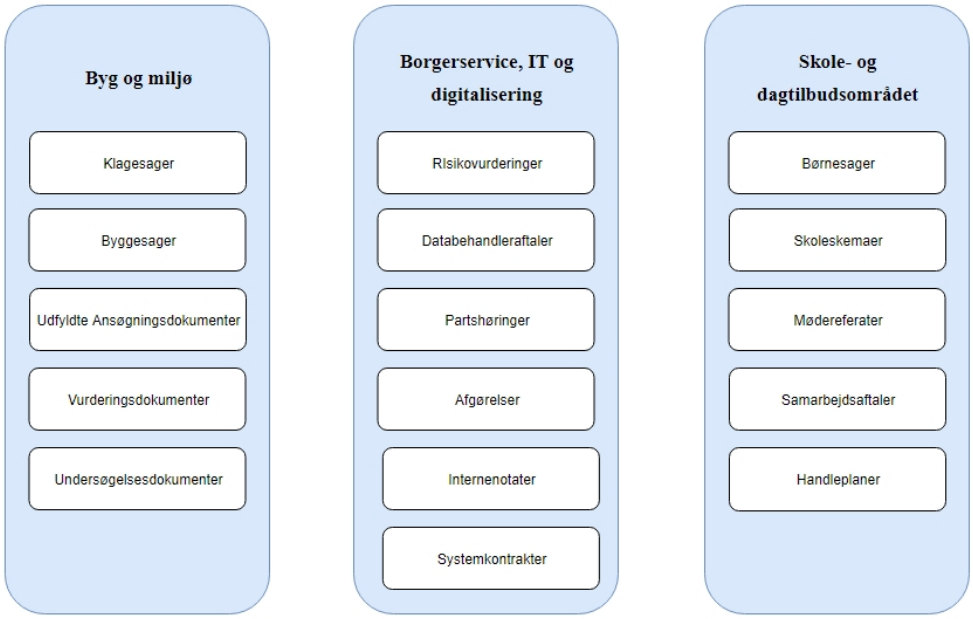
Eksempel på journalisering:

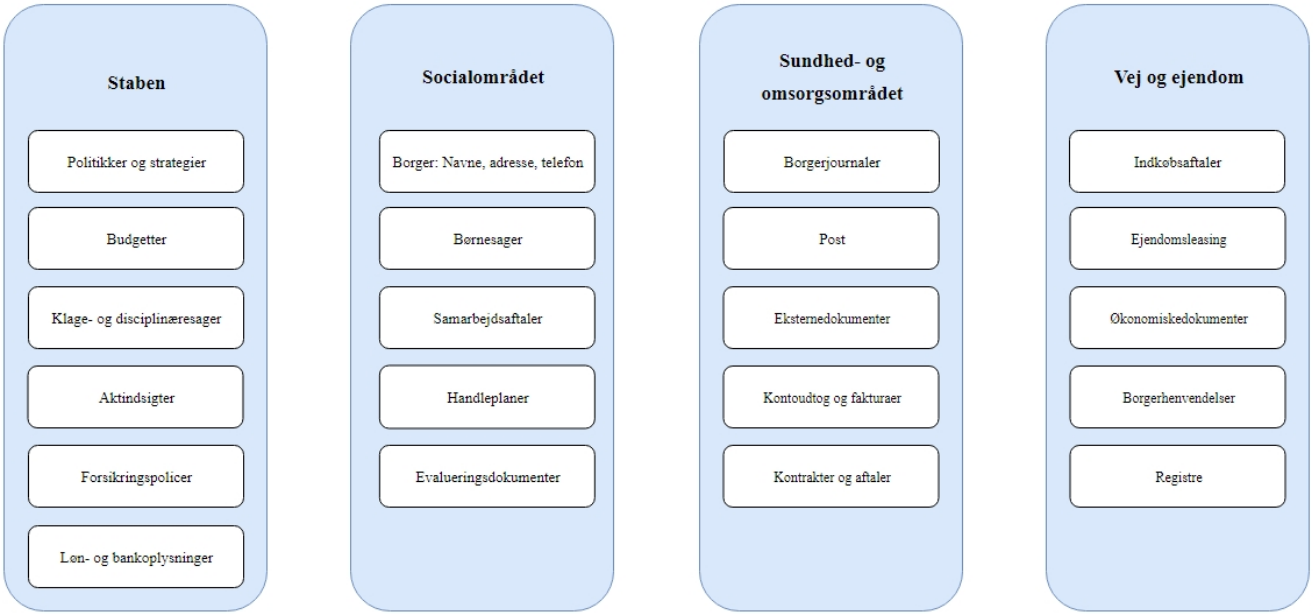
Sagstitel: Risikovurderinger – KMD – Kommunernes Sygedagpengesystem (KSD) – 2020
Journalkode: 85.10.18
Handlingsfacet: P30

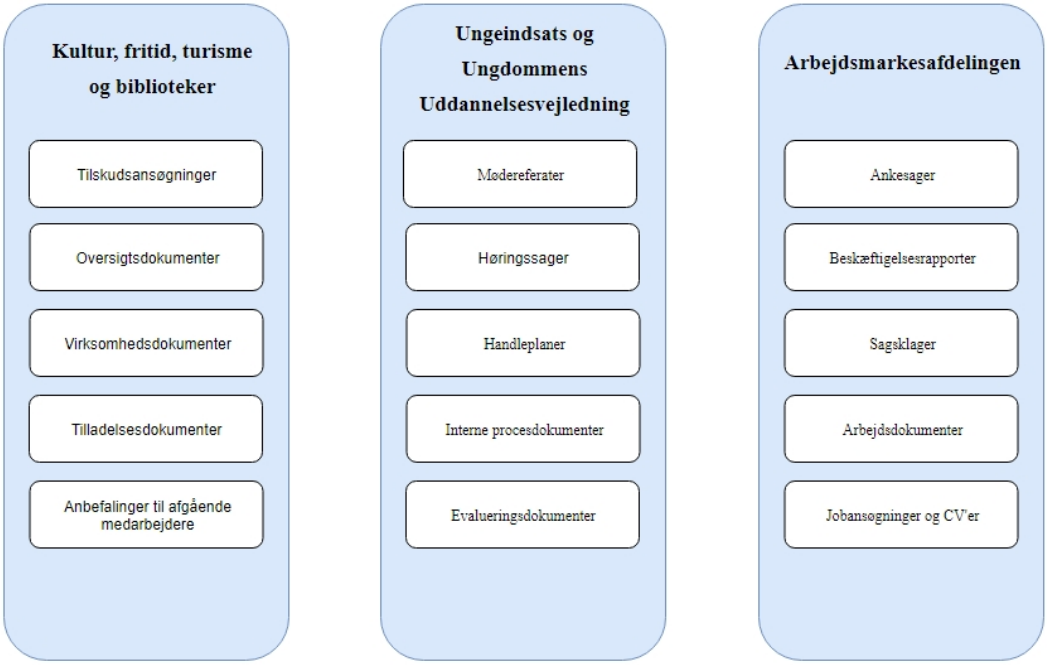
UDKAST

Bilag 2 – Eksempler på afdelingernes informationsaktiver

Informationsaktivsoversigten lister eksempler på hvilke informationsaktiver, som findes i kommunen områder. De oplistede aktiver er eksempler og ikke udtømmende. Nogle aktiver vil gå igen i samtlige områder (uden at være listet i eksemplerne), herunder aktindsigter og budgetter.




Staben
Politikker og strategier
Budgetter
Klage- og disciplinæresager
Aktindsigter
Forsikringspolicer
Løn- og bankoplysninger
Socialområdet
Borger: Navne, adresse, telefon
Børnesager
Samarbejdsaftaler
Handleplaner
Evalueringsdokumenter
Sundhed- og omsorgsområdet
Borgerjournaler
Post
Eksternedokumenter
Kontoudtog og fakturaer
Kontrakter og aftaler
Vej og ejendom
Indkøbsaftaler
Ejendomsleasing
Økonomiskedokumenter
Borgerhenvendelser
Registre


Kultur, fritid, turisme og biblioteker
Tilskudsansøgninger
Oversigtsdokumenter
Virksomhedsdokumenter
Tilladelsesdokumenter
Anbefalinger til afgående medarbejdere
Ungeindsats og Ungdommens Uddannelsesvejledning
Mødereferater
Høringssager
Handleplaner
Interne procesdokumenter
Evalueringsdokumenter
Arbejdsmarkesafdelingen
Ankesager
Beskæftigelsesrapporter
Sagsklager
Arbejdsdokumenter
Jobansøgninger og CV'er

Bilag 3 – Trusselsoversigt

Trusselsoversigten lister en række risikoscenarier til inspiration. Der er foretaget en central vurdering af sandsynligheden og konsekvenserne for kommunen generelt, som man kan tage udgangspunkt i. Konsekvenserne er opdelt på fortrolighed, integritet og tilgængelighed, med udgangspunkt i konsekvensklassifikationen (se s.7). Husk, der laves kun vurderinger af sandsynlige scenarier.

Oversigten er senest opdateret november 2019.

Fysiske og miljømæssige trusler	Sandsynlighed (S)	Fortrolighed (F)	Integritet (I)	Tilgængelighed (T)
Brandskade				
Bybrand, brand i tilstødende bygninger eller faciliteter	1	1	3	3
Elektrisk brand forårsaget af el-installation, kortslutninger	1			
Brand forårsaget af skødesløshed eller forsømmelse	2			
Eksplosion i tilstødende bygninger eller faciliteter	1			
Fejl i forbindelse med drifts-, support- eller vedligeholdelseprocesser	2			
Kølingsfejl, luftfiltreringsfejl, opvarmningsfejl	1			
Brandstiftelse, hærværk	2			
Serviceleverandørfejl, hostingleverandørfejl	3			
Fejl hos underleverandører, dårlig håndtering af underleverandører	2			
Vandskade				
Rørskade, kloakoversvømmelse, sprinklersystemfejl	1	1	3	3
Digebrud, flodbølge	1			
Kraftigt regnfald, der resulterer i oversvømmelse	2			
Kraftigt snefald	1			
Storm, orkan	1			
Elektromagnetisk beskadigelse				
Lynnedslag, elektromagnetisk puls	2	1	3	3
Solstorm, elektromagnetisk stråling	1			
Statisk elektricitet	1			
Skade ved naturhændelse				
Jordskælv	1	1	2	3
Kuldebølge, frost	1			
Hedebølge, tørke	2			
Skade ved katastrofal ulykke				
Fly-, tog- eller lastvognsulykke	1	1	2	3
Eksplosion i tilstødende bygninger eller faciliteter	1			
Terrorbombning	1			
Forurening af faciliteter				
Bybrand, brand i tilstødende bygninger eller faciliteter	1	1	2	3
Radioaktivt udslip fra atomulykke	1			
Kemisk udslip, gasudslip	1			
Luftbårne partikler, vulkansk nedfald, støv	1			
Biologisk eller kemisk udslip	1			

Bruger og it-driftsmæssige trusler	S	F	I	T
Brugerfejl				
Uforsætlige brugerhandlinger, fejlbehandling af medier, mangel på brugerud-dannelse	3	2	1	1
Drifts- eller vedligeholdelsesfejl				
Fejl i forbindelse med drifts-, support- eller vedligeholdelsesprocesser	1	3	3	3
Angreb med skadelig kode				
Virus, malware, ransomware, rootkits, ondsindede links og trojanske heste	2	3	3	3
Cyberangreb				
Destruktiv hacking, hacktivisme	2	3	3	3
DDoS- eller SPAM-angreb	2			
Statsfinansierede angreb	1			
Forfalskning af informationer, ødelæggelse af hjemmesider	1			
Hacking, industrispionage, aflytning, opsnapning af information	2			
Kapacitetsfejl				
Kapacitetsmangel for systemer eller storage	2	1	2	3
Softwarefejl				
Softwarenedbrud, bugs, databasekorruption	2	3	3	3
Uautoriseret eller ikke-testet kode	1			
Hardware fejl				
Kommunikationslinjenedbrud	2	1	3	3
Udstyrsnedbrud eller -defekt, slid, korrosion, henfald af lagringsmedier	2			
Fejl i fysisk miljøstyring				
Kølingsfejl, luftfiltreringsfejl, opvarmningsfejl	1	1	2	3
Vandforsyningssvigt	1			
El-forsyningsfejl				
Strømsvigt, el-forsyningslinjebrud	2	1	2	3
Strømfluktuation, sag, surge, spike, brownout	2			
Forsyningsudstyrssvigt, UPS-fejl, generatorfejl	1			
Elforsyningsoverbelastning	2			

Misbrug eller brud på fortrolighed	S	F	I	T
Misbrug				
Forfalskning, svindel, underslæb	1	4	4	2
Uautoriseret brug, misbrug af rettigheder	2			
Brud på ophavsrettigheder	1			
Tilsigtet informationslæk eller -tyveri				
Hacking, industrispionage, aflytning, opsnapning af information	2	4	2	1
Tyveri af datamedier	1			
Politisk eller økonomisk motiveret informationslæk	1			
Utilsigtet informationslæk				
For vidtgående brugerrettigheder/adgangsprivilegier	2	4	2	1
Forkert konfigureret adgangskontrol	1			
Fejlagtig publicering af data, der indeholder følsomme oplysninger	2			
Tab af datamedier eller fysiske dokumenter	2			
Bevidst ødelæggelse af aktiver				
Brandstiftelse	2	4	4	4
Terrorbombning	1			
Sabotage begået af hævngærrige medarbejdere	1			
Tyveri af fysiske aktiver				
Indbrud, røveri	1	3	2	2

Tyveri, tricktyveri	2			
Tyveri begået af ansatte	1			
Straf for manglende overholdelse				
Brud på ophavsrettigheder	1			
Virksomheden opfylder ikke de gældende compliance-krav	3	3	2	1
Forkert offentliggørelse af personlige oplysninger	1			

Arbejdshindring og personalerelaterede trusler	**S**	**F**	**I**	**T**
Videnstab				
Afskedigelse, opsigelse, rekruttering fra konkurrenter	3			
Manglende vidensoverførsel	3	1	1	2
Personafhængighed	3			
Tab af personale				
Vold, bortførelse, mord	1			
Dødsulykke eller alvorlige skader	1	1	1	3
Sygdom, epidemi, pandemi	2			
Arbejdsafbrydelse				
Lokale arbejdskonflikter, strejke, lockout	1	1	1	4

Leverandørrelaterede trusler	**S**	**F**	**I**	**T**
Leverancesvigt				
Konkurs, nedlæggelse	1			
Serviceleverandørfejl, hostingleverandørfejl	2			
Afvigelse fra aftalt serviceniveau/leverede ydelser	2	1	2	4
Ændringer af servicen, en ny strategi fra leverandøren	1			
Fejl hos underleverandører, dårlig håndtering af underleverandører	1			
Sikkerhedsbrud fra leverandørens side				
Ondsindede medarbejdere, udnyttelse af privilegier	1	4	4	4
Utilstrækkelig sikkerhed fra leverandørens side	1			
Leverandørafhængighed				
Egne/ikke-standardløsninger, dårlige muligheder for dataeksport	3	1	3	4
Lange kontraktperioder, høj pris for at afbryde samarbejde	2			
Leverandør mangler compliance- eller governance-procedurer				
Leverandøren opfylder ikke virksomhedens sikkerhedspolitik og -regler	2	3	3	2
Leverandøren opfylder ikke de relevante compliance-krav	2			

Trusler knyttet til store ændringer eller implementeringer	**S**	**F**	**I**	**T**
Introduktion af nye og ubehandlede sikkerhedstrusler				
Virksomheden opfylder ikke de gældende compliance-krav	3	3	3	2

Bilag 4 – Eksempler på risici for den registrerede

Når Norddjurs Kommune foretager en risikovurdering af konsekvenserne for den registreredes rettigheder og frihedsrettigheder, skal det indtænkes, hvilken trussel eller skade, en behandling kan forvolde. Nedenfor er listet eksempler på risici, som man bør have med i sine overvejelser ved en risikovurdering af de registreredes rettigheder.

Følgende er eksempler på behandlinger, hvor behandlingen kan indebære risici for de registreredes rettigheder og frihedsrettigheder:

- Behandling af børneoplysninger
- Behandling af sårbare personer
- Behandling af sensitive data omhandlende race
- Behandling af sensitive data omhandlende etnisk oprindelse
- Behandling af sensitive data omhandlende politiske meninger
- Behandling af sensitive data omhandlende religiøs overbevisning
- Behandling af sensitive data omhandlende filosofisk overbevisning
- Behandling af sensitive data omhandlende foreningstilknytning
- Behandling af sensitive data omhandlende helbredsoplysninger
- Behandling af sensitive data omhandlende seksuelle forhold
- Behandling af sensitive data omhandlende seksuel orientering
- Behandling af sensitive data omhandlende kriminelle domme eller forbrydelser
- Behandling af større mængder af informationer, som påvirker flere personer
- Automatisk behandling som profiling, der giver grundlag for beslutninger med lovmæssig effekt eller lignende effekt
- Større skala af systematisk overvågning af offentlige rum
- Brug af ny teknologi

Eksempler på trusler forbundet med en behandling:

- Oplysninger går tabt
- Oplysninger bliver stjålet
- Oplysninger bliver slettet
- Oplysninger bliver ændret
- Ulovlig og overdreven indsamling af oplysninger af den dataansvarlige eller databehandleren
- Brug og opbevaring af ukorrekte og forældede oplysninger
- Uhensigtsmæssig brug eller misbrug af oplysninger
- Brug af oplysninger til behandlinger udover de registreredes forventninger
- Ualmindelig brug af oplysninger udover sociale normer – hvor en behandling strider imod sund fornuft
- Ulovlig indblanding eller beslutningstagning, som organisationen ikke kan begrunde
- Ulovlig eller uautoriseret adgang til oplysninger
- Ulovlig eller uautoriseret deling af oplysninger til andre dataansvarlige eller databehandlere
- Ulovlig eller uautoriseret overførsel af oplysninger til usikre tredjelande eller internationale organisationer
- Ulovlig eller uautoriseret videregivelse af oplysninger til forkerte modtagere
- Ulovlig eller uautoriseret offentliggørelse af oplysninger

Eksempler på skader for de registreredes rettigheder:

Fysiske skadestyper:

- Fysisk skade på personer (herunder også tab af retten til livet)
- Tab af frihed
- Tab af bevægelsesfrihed

- Skade til indtjening
- Finansielle tab (tabt ret til ydelser, fx kontanthjælp, dagpenge el. boligstøtte)

Ikke-fysiske skadestyper:

- Skade pga. overvågning eller eksponering af identitet
- Skade pga. overvågning eller eksponering af karakteristika
- Skade pga. overvågning eller eksponering af handlinger
- Skade pga. overvågning eller eksponering af foreninger
- Skade pga. overvågning eller eksponering af holdninger
- Nedsat ytringsfrihed
- Skade på omdømme
- Skade på personligt omdømme
- Skade på familieomdømme
- Skade på en arbejdsplads omdømme
- Social angst
- Forlegenhed
- Frygt
- Uacceptabel indtrængen i privatlivet
- Diskrimination
- Tab af retten til retfærdig rettergang
- Stigmatisering
- Tab af autonomi
- Begrænsning af personlige valg
- Identitetstyveri
- Berøvelse af kontrol over egne personlige oplysninger