Næstved Kommune

Informationssikkerhedspolitik
ISO 27001

Versionsdato:
15. marts 2018

Baggrund

Nærværende dokument beskriver governance for Næstved Kommunes informationssikkerhedspolitik. Hensigten med politikken er at skabe rammerne for, at al anvendelse og behandling af informationer i Næstved Kommune sker efter gældende lovgivning, anerkendte standarder og øvrige regelsæt, samt at alle medarbejdere har en sikkerhedsorienteret adfærd og en bevidst holdning til begrebet informationssikkerhed. Informationssikkerhedspolitikken er baseret på ISO 27001 standarden.

Den nationale strategi for cyber- og informationssikkerhed (2014) stiller krav til statslige myndigheder om at implementere og arbejde systematisk efter sikkerhedsstandarden ISO 27001. Med den seneste fællesoffentlige digitaliseringsstrategi (2016-2020) er den øvrige del af den offentlige sektor nu underlagt et krav om at følge principperne i standarden.

Med en systematisk tilgang til styring af risici, kan organisationen investere i informationssikkerhed, hvor det giver størst muligt afkast – hvad enten det indebærer beskyttelse af organisationens fysiske rammer, it-tekniske kontroller eller en ændring af medarbejdernes adfærd.

Det er informationssikkerhedspolitikken, som overordnet skal godkendes politisk. Herefter skal Informationssikkerhedshåndbogen (ISO 27002) efterfølgende indarbejdes i administrationen således at den operationelle udmøntning af Informationssikkerhedspolitikken efterleves, herunder bl.a. den ny lovgivning om Persondataforordningen (GDPR). Informationssikkerhedspolitikken erstatter sammen med den kommende informationssikkerhedshåndbog den tidligere it-sikkerhedspolitik DS484.

I regi af Digitaliseringsforeningen Sjælland (DIGIT) samarbejder Næstved Kommune med de øvrige medlemskommuner i projektet vedr. informationssikkerhedshåndbogen. Resultatet af dette samarbejde indarbejdes løbende i Næstved Kommunes egen Informationssikkerhedshåndbog.

Næstved Kommunes Informationssikkerhedspolitik er udarbejdet med øje på andre kommuners arbejde og best pratice på området. Dette er bl.a. sikret af Næstved Kommunes samarbejde med BDO IT-revision, som udfører revision på området i flere af landets kommuner. Da Næstved Kommune arbejder efter ISO-standardens opbygning og principper med mulighed for en evt. certificering, har det været formålstjenstligt at dokumentet allerede er opbygget efter standardens kapitelinddelinger. Dette er bl.a. baggrunden for at nærværende dokument starter med kapitel 4, og ikke kapitel 1.

Når databeskyttelsesforordningen træder i kraft den 25. maj 2018, er der mange regler, som også kommunens databehandlere og medarbejdere skal overholde. For at skabe bedre forståelse og hjælp til at overholde disse regler fx i relation til behandlingsaktiviteter, vil kommunen inden 25. maj udarbejde og indføre et lokalt adfærdskodeks og nogle principper for god og forsvarlig databehandling. Adfærdskodekset vil være et nyttigt redskab til at implementere forordningens krav i praksis.

Det lokale adfærdskodeks skal ses som en måde til, at understøtte organisationen i at efterleve reglerne fra databeskyttelsesforordningen. Det er den enkelte systemejer eller dataejer, der skal sikre overholdelse af adfærdskodekset. Derfor vil det blive understøttet med ledelsesinformation og andre former for opfølgning. Adfærdskodekset behandles og godkendes af kommunens Informationssikkerhedsudvalg.

Informationspolitikken skal revurderes en gang om året på baggrund af en risikoanalyse, der vurderer trusler, konsekvenser og risici ved kommunens kritiske informationssystemer. En revideret informationssikkerhedspolitik forelægges derfor Byrådet i december 2018.

Indhold

4 Organisationens kontekst

4.1 Forståelse af organisationen og dens kontekst

Dokumentation af organisationen http://erna.naestved.dk/Organisation/NaestvedKommune.aspx

Kontekst

Informationsbehandling i Næstved Kommune har et sikkerhedsniveau, som tilgodeser lovgivningskrav og myndighedsforventninger og muliggør en bredspektret informationssystemanvendelse.

Informationssikkerhedspolitikken skal skabe rammerne for en sikker informationsbehandling for både borgere, brugere, virksomheder og samarbejdspartnere samt medarbejdere, ledelse og politikere i Næstved Kommune.

Informationssikkerhedspolitikken fastsætter hovedprincipperne for governance af informationssikkerheden, herunder placering af ansvar for varetagelse af informationssikkerheden.

Den overordnede informationssikkerhedspolitik er uddybet i en informationssikkerhedshåndbog samt en række bilag, som det fremgår i Næstved Kommunes Information Security Management System – efterfølgende benævnt ISMS

Bilagene er opdelt i 4 kategorier:

- Retningslinier for it-medarbejdere.
- Retningslinier for brugere.
- Retningslinier for systemejere.
- Retningslinier for eksterne samarbejdspartnere.

Som supplement til Informationssikkerhedspolitikken - med det formål, at skabe en effektiv formidling af budskabet - er der udarbejdet kort og præcis brugerinfo: "Sikker it i Næstved Kommune" og systemejerinfo: "Vejledning til systemejere".

Informationssikkerhedspolitikken, Informationssikkerhedshåndbogen og relevante bilag, er tilgængelige på kommunens Secure ISMS
https://nstvedkommune1.saas.neupart.com/authenticate?redirectto=/main/security/redirect

Sikkerhedspolitikken tilstræber at være realistisk, operationel, logisk, acceptabel og kontrollerbar.

Kommunen skal satse på sikre løsninger, høj driftstabilitet, enkelthed og informationsløsninger som er integrerede.

Med dette udgangspunkt er informationssikkerhedsniveauet fastsat og beskrevet i informationssikkerhedspolitikken.

Informationssikkerhedspolitikken tilstræber, at informationsbehandling har en høj kvalitet, er effektiv, er sikker og er målrettet de konkrete opgaver, som kommunen udfører. For at sikre informationsbehandling, ønsker Næstved Kommune, at alle medarbejdere har en sikkerhedsorienteret kultur og en bevidst holdning til begrebet informationssikkerhed, hvor der lægges vægt på reel sikkerhed frem for formel sikkerhed.

4.2 Forståelse af interessenters behov og forventninger

Formålet med Informationssikkerhedspolitikken er at fastlægge informationssikkerheden på et overordnet niveau samt sikre implementeringen af de nødvendige retningslinjer, procedurer og kontroller i organisationen. Desuden ønskes en høj driftssikkerhed og at gældende lovgivning og myndighedskrav overholdes.

Næstved Kommunes informationssikkerhedsniveau er resultatet af den samlede mængde af normer, foranstaltninger og kontroller, der skal sikre organisationens driftsmæssige kontinuitet og minimere de økonomiske risici ved tab, minimere misbrug af organisationens informationer samt undgå at borgernes tillid svækkes og kommunens omdømme skades.

Det er kommunens ledelse, der har ansvaret for informationssikkerheden, herunder sikring af *tilgængelighed*, *fortrolighed* og *integritet*.

I forbindelse med en gennemført risikovurdering af kommunens informationsbehandling, er der blevet kortlagt en række risici, som informationssikkerhedspolitikken skal medvirke til at reducere. Informationssikkerhedspolitikken skal således sikre

- at informationssikkerheden etableres på et effektivt og ensartet niveau, så risikoen for alvorlige fejl begrænses,

- høj driftssikkerhed og tilgængelighed til systemer,
- at datagrundlaget for kommunens forretningsgange er retvisende,
- at informationssikkerheden er tilpasset de værdier og informationer, som skal beskyttes,
- at væsentlige data og værdier ikke går tabt,
- at informationssikkerheden indarbejdes i de eksisterende forretningsgange,
- at ansvaret er entydigt placeret,
- at data ikke bliver tilgængelige for uvedkommende.

> Informationssikkerhedspolitikken skal i overensstemmelse med kommunens vitale forretningsgange være en afvejning af væsentlighed og risiko. Sikringen skal stå mål med risikoen. Vi vil ikke sikre os for enhver *pris*, men være bevidst om enhver *risiko*.

Endvidere har en effektiv og konsekvent formidling af informationssikkerhedspolitikken til formål, at skærpe brugernes opmærksomhed på sikkerhed i forbindelse med anvendelse af de forskellige systemer ligesom informationssikkerhedspolitikken skal sikre, at alle brugere er beskyttet af et entydigt regelsæt.

4.3 Bestemmelse af omfanget af ledelsessystemet for informationssikkerhed

Omfang af informationssikkerhedspolitik

Informationssikkerhedspolitikken omfatter alle kommunens forretningsgange, systemer og data i kommunens besiddelse. Informationssikkerhedspolitikken gælder for alle ansatte i kommunen, samt leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til kommunens systemer og data,

Dokumentation af anvendelsesområdet for ISMS

Informationssikkerhedspolitikken, Informationssikkerhedshåndbogen og bilagene omfatter alle brugere af kommunens administrative informationssystemer og informationsbaserede infrastruktur. Endvidere regulerer informationssikkerhedspolitikken øvrige områder, hvor der sker digitalt og manuel behandling af administrative data.

I det omfang Næstved Kommune udliciterer it-driftsafviklingen til eksterne leverandører skal det sikres, at serviceleverandøren overholder retningslinjerne, som de er beskrevet i informationssikkerhedspolitikken, Informationssikkerhedshåndbogen og relevante bilag således, at informationssikkerhedsniveauet er i overensstemmelse med Næstved Kommunes informationssikkerhedspolitik.

4.4 Ledelsessystem for informationssikkerhed

Informationssikkerhedsprocessen

Næstved Kommunes ledelsessystem er baseret på en løbende risikobaseret tilgang, hvor der løbende foretages en evaluering af sikkerhedstiltag med henblik på fortsat, at have et for kommunen korrekt informationssikkerhedsniveau.

5 Lederskab

5.1 Lederskab og engagement

Næstved Kommunes øverste ledelse skal støtte Kommunens informationssikkerhedspolitik ved at udlægge klare retningslinjer, udvise synligt engagement samt sikre en præcis placering af ansvar.

Informationsbehandlingen i Næstved Kommune har til formål at understøtte kommunens overordnede vision. Kommunens digitaliseringsstrategi beskriver visioner, mål og handleplaner for informationsbehandlingen. Informationssikkerhedspolitikken skal medvirke til at danne grundlag for, at digitaliseringsstrategien og de konkrete handleplaner kan effektueres.

Informationssikkerhedspolitikken skal endvidere sikre, at informationsbehandlingen opfylder alle sikkerhedskriterier, som forventes opfyldt af en offentlig forvaltning.

5.2 Politik

Distribution af informationssikkerhedspolitikken

Informationssikkerhedspolitiken og Informationssikkerhedshåndbogen gøres tilgængeligt fra kommunens intranet ved link til kommunens Secure ISMS, som er tilgængelig for alle medarbejdere med gyldig login konto på kommunens netværk.

Revision af informationssikkerhedspolitikken

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

- Informationssikkerhedspolitikken
- Informationssikkerhedshåndbogen inkl. bilag
- Systemejer og dataejer oversigter.

Informationssikkerhedspolitikken skal revideres ved lovgivningsmæssige eller væsentlige organisatoriske ændringer.

Ændringer i informationssikkerhedspolitikken godkendes af Økonomiudvalget, mens ændringer i Informationssikkerhedshåndbogen godkendes af direktionen.

Opfølgning på implementering af sikkerhedspolitikken

Der foretages løbende opfølgning på, hvorvidt reglerne i Informationssikkerhedshåndbogen samt bilagene, i praksis efterleves. Informationssikkerheden kontrolleres ud fra en konkret vurdering af væsentlighed og risiko. Øverste sikkerhedsansvarlige har ansvaret for, at denne opfølgning foretages mindst en gang om året eller ved større tekniske eller organisatoriske ændringer. Opfølgningen kan evt. foretages med ekstern bistand.

Vedligeholdelse af sikkerhedspolitik

Næstved kommunes Informationssikkerhedsudvalg er ansvarlig for at oprette, vedligeholde og distribuere Informationssikkerhedspolitikken, Informationssikkerhedshåndbogen samt bilag.

5.3 Roller, ansvar og beføjelser i organisationen

Sikkerhedsorganisation

Med henblik på at sikre kommunens informationsbehandling, er der etableret en entydig informationssikkerhedsorganisation. I skemaet på næste side er informationssikkerhedsorganisationen og dennes ansvar og roller beskrevet.

Dette ændrer **ikke** ved det til enhver tid gældende ledelsesansvar indenfor kommunens almindelige organisatoriske ledelseshierarki, herunder også ansvaret for formidling af Informationssikkerhedspolitik, -håndbog og tilhørende bilag til medarbejdere i egen organisation.

Ansvar og bemyndigelse i forbindelse med informationssikkerhed

Opgaven er i praksis uddelegeret til Informationssikkerhedsudvalget. Ajourføring skal mindst finde sted en gang årligt eller ved større omlægninger i informationsbehandlingen.

Roller og ansvar fremgår i Informationssikkerhedshåndbogens kapitel 6.

Benævnelse	Placering og forklaring	Ansvar
Øverste sikkerhedsansvarlige	Kommunaldirektøren	Er øverste sikkerhedsansvarlig. Er ansvarlig for den overordnede tilrettelæggelse af informationssikkerheden i kommunen, herunder ansvaret for opfølgning og kontrol. Opgaven med sikring af og opfølgning på kommunens informationssikkerhed er uddelegeret til Informationssikkerheds-koordinatoren.
Informationssikkerheds-koordinator	Organisatorisk tilknyttet Center for Politik og Udvikling, Team Strategi og Digitalisering	Fungerer som øverste sikkerhedsansvarliges stedfortræder i forbindelse med sikring af og opfølgning på kommunens informationssikkerhed. Informationssikkerheds-koordinatoren er uafhængig af IT-driftsorganisationen og refererer direkte til kommunens øverste sikkerhedsansvarlige og direktion ifbm. med informationssikkerhedsspørgs-mål. Rapportering af informationssikkerhedshændel-ser sker ligeledes direkte til øverste sikkerhedsansvarlige og direktion. Ansvarlig for vedligeholdelse af informationssikkerhedspolitik og Informationssikkerheds-håndbogen. Ansvarlig for Kommunens Information Security Management System (ISMS)
Informationssikkerheds-udvalg (styregruppen)	Informationssikkerhedsudvalgets sammensætning skal afspejle kommunens opbygning og organisatoriske struktur. Udvalget er sammensat af: • Kommunaldirektøren • En Centerchef • En juridisk kompetence • En fagcenterchef • En virksomhedsleder • En IT-kompetence på lederniveau • En repræsentant for DIGIT og Digitalisering på lederniveau • Informationssikkerhedskoordi	Med udgangspunkt i oplæg fra Informationssikkerheds-koordinatoren: At koordinere og prioritere Informationssikkerheds-arbejdet At fastsætte Informationssikkerhedsmål og relaterede informationssikker-hedskontroller. At fungere som sparringspartnere for Informationssikkerheds-koordinatoren i Informationssikkerheds-spørgsmål.

	natoren	Beslutningskompetencerne er besluttet, at være på embedsmandsniveau, men udvalget står til ansvar overfor Økonomiudvalget samt Byrådet.
Systemejer	Alle systemer tilhører en systemejer, der er forvaltningsdirektør, kontorchef eller afdelingschef, som med udgangspunkt i et fagligt ansvar anskaffer et Informationssystem til at understøtte opgavevaretagelsen. Opgaven som systemejer kan uddelegeres helt eller delvist i en række underliggende roller nærmere beskrevet i kapitel 8. Ansvaret kan ikke uddelegeres.	Udarbejdelse af instrukser for de enkelte systemer. Udarbejdelse af uddybende systemdokumentation Beskrivelser af relaterede interne kontroller – elektroniske og manuelle Etablering af systemsupport Administration af leverandøradgang Supplerende opgaver i forbindelse med systemanvendelsen herunder autorisation, logning, interne kontroller, udvikling og anskaffelse samt nødberedskab
Dataejer	Udpeges af systemejer. Er en fagchef/teamleder, der står som ejer af delproces og har personaleansvar for medarbejdere i processen. Der kan være flere dataejere for hvert system.	Dataejeren har ansvaret for, at retningslinjer og instrukser for et systems anvendelse overholdes af medarbejderne Dataejer skal føre tilsyn og kontrol med, at retningslinjer og instrukser følges
Systemadministrator	Navngiven systemadministrator – typisk en kontorchef eller medarbejder med særligt kendskab, som har ansvaret for at udføre opgaver uddelegeret af systemejer. Rollen kan underopdeles i flere roller. • Kontraktejer • Budgetejer • Autorisationsejer • Teknikejer • Sikkerheds- og controllerejer	Udarbejdelse af instrukser for de enkelte systemer. Udarbejdelse af uddybende systemdokumentation Beskrivelser af relaterede interne kontroller – elektroniske og manuelle Etablering af systemsupport Administration af leverandøradgang Supplerende opgaver i forbindelse med systemanvendelsen herunder autorisation, logning, interne kontroller, udvikling og anskaffelse samt nødberedskab

6 Planlægning

6.1 Handlinger til håndtering af risici og muligheder

6.1.1 Generelt

Informationssikkerhedspolitikken har udgangspunkt i god informationsskik, best-practice samt lovgivning indenfor informationssikkerhed "*Databeskyttelsesloven*". Informationssikkerhedspolitikken er udarbejdet med ISO27001:2013 Standard for informationssikkerhed, som referenceramme.

Konsekvensvurdering

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

6.1.2 Vurdering af informationssikkerhedsrisici

Informationssikkerhedsniveauet er fastlagt på baggrund af en informationsrisikovurdering således, at informationssikkerheden er afstemt efter betydningen af kommunens data og systemer. Som udgangspunkt er det hensigten, at informationssikkerheden skal være på et niveau, hvor der aldrig skabes tvivl om, hvorvidt kommunens informationssikkerhed er betryggende.

Der gennemføres opfølgning på risikovurderingen mindst en gang om året - eller ved større tekniske eller organisatoriske ændringer - således, at kommunens ledelse kan holdes orienteret om det aktuelle risikobillede.

Der gennemføres løbende opfølgning og kontrol på kommunens informationssikkerhed. Dette omhandler både at sikre at den nødvendige dokumentation findes, og at den følges i praksis.

6.1.3 Håndtering af informationssikkerhedsrisici

Risikohåndtering

Der skal indføres passende sikringstiltag baseret på risikovurderingen

Det valgte sikringstiltag skal sammenholdes med sikringstiltagene anført i Informationssikkerhedshåndbogen for at sikre, at ingen nødvendige kontroller udelades.

Der skal udarbejdes en Statement of Applicability (SoA) baseret på de valgte sikringstiltag

SoA skal omfatte begrundelsen for at medtage eller fravælge kontrolforanstaltninger.

Vi behandler risici ved hjælp af en eller flere af de fire muligheder.

- Accepterer risici
- Reducerer risici ved at implementere kontroller
- Dele risici
- Undgå risici

6.2 Informationssikkerhedsmålsætninger og planlægning for opnåelse heraf

Informationssikkerhedsmål

Næstved 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 Næstved Kommune

Målsætningerne for informationssikkerhed skal være:

- i overensstemmelse med informationssikkerhedspolitikken
- målbare, hvor det er muligt
- kommunikerede
- regelmæssigt opdaterede

Informationssikkerhedsmålene skal dokumenteres struktureret og ensartet.

7 Support

7.1 Ressourcer

Sikring af ressourcer til ISMS'et

Ledelsen skal sikre, at der afsættes tilstrækkelige ressourcer til at holde ISMS'et kørende

7.2 Kompetencer

Tilstrækkelige kompetencer til at drive ISMS'et

Organisationen skal sikre, at de personer, der er ansvarlige for ISMS'et har de nødvendige kompetencer

Hvis ikke alle nødvendige kompetencer er til stede i organisationen, skal der tages initiativ til at tilegne sig disse kompetencer.

Organisationen skal kunne dokumentere, at de relevante kompetencer er til rådighed.

7.3 Bevidsthed

Uddannelse i sikkerhedspolitikken

Næstved Kommunes informationssikkerhedspolitik vedrører den samlede administrative systemanvendelse og det samlede informationsflow. Gennemførelse af informationssikkerhedspolitikken skal derfor finde sted med bistand fra brugere og medarbejdere i kommunen.
Alle kommunens medarbejdere har et ansvar for at bidrage til en sikker og betryggende informationsbehandling.

En effektiv og konsekvent formidling af informationssikkerhedspolitikken skal skærpe brugernes opmærksomhed på sikkerhed i forbindelse med anvendelse af de forskellige systemer.

Som brugere af Næstved Kommunes systemer og data, skal alle administrative brugere følge Informationssikkerhedspolitikken, Informationssikkerhedshåndbogen og relevante bilag. Systemer og data må udelukkende anvendes til udførelse af de relevante arbejdsopgaver og systemer og data skal beskyttes i overensstemmelse med deres indhold og følsomhed.

Ansvaret for at efterleve sikkerheden omkring informationsbehandlingen i Næstved Kommune, er placeret hos den enkelte medarbejder. Det skal derfor fremhæves, at overtrædelse af Informationssikkerhedspolitikken samt relaterede bilag, efter omstændighederne, kan medføre sanktioner.

Hvis en medarbejder opdager trusler imod kommunens informationsbehandling eller er bekendt med overtrædelser af informationssikkerhedspolitikken, skal dette altid meddeles nærmeste leder, der efterfølgende er forpligtiget til at informere Informationssikkerhedskoordinatoren hurtigst muligt.

7.4 Kommunikation

Kommunikation om informationssikkerhed

Organisationen skal fastlægge en kommunikationsplan for informationssikkerhed. Kommunikationsplanen for informationssikkerhed skal beskrive:

- hvad der skal kommunikeres
- hvornår der skal kommunikeres
- modtagere
- hvem, der skal kommunikere
- hvordan kommunikationen skal foretages (medie/form)
- Dokumenteret information

7.5 Dokumenteret information

7.5.1 Generelt

Dokumentation af informationssikkerhed

Secure ISMS-dokumenter omfatter:

- Overordnet Informationssikkerhedspolitik for Næstved Kommune
- Informationssikkerhedspolitik og -målsætninger
- Informationssikkerhedshåndbog
- Bilag til Informationssikkerhedshåndbogen
- Statement of Applicability
- Risikovurderingsrapport (skal udarbejdes)
- Risikohåndteringsplan (skal udarbejdes)
- Beredskabsplan for Team servicedesk og IT

Den nødvendige dokumentation for effektiviteten af ISMS'et kan omfatte:

- resultater af uddannelse, kompetencer, erfaring og kvalifikationer
- resultater af overvågning og måling
- intern audit
- resultater af intern audit
- resultater af ledelsesberetningen
- resultater af korrigerende handlinger

Dokumentationen bør opbevares i Næstved kommunes ESDH system.

7.5.2 Udarbejdelse og opdatering af information

Vedligeholdelse af informationssikkerhedsdokumenter og -registreringer

Informationssikkerhedspolitikken er udarbejdet af Team servicedesk og IT og er kvalitetssikret af Informationssikkerhedsudvalget, der i udarbejdelsesprocessen har fungeret som styregruppe for ISO27001-projektet.

Ændringer i Informationssikkerhedspolitikken besluttes af Økonomiudvalget, mens ændringer i Informationssikkerhedshåndbogen godkendes af direktionen. Ændringer i operationelle procedurer kan foretages i de ansvarlige Centre, afdelinger eller virksomheder.

Informationssikkerhedsdokumenter og -registreringer skal være klart identificerede (beskrivelse, titel, dato, forfatter, nummer).

Informationssikkerhedsdokumenter og -registreringer skal godkendes inden offentliggørelse.

7.5.3 Styring af dokumenteret information

Håndtering af informationssikkerhedsdokumenter og -registreringer

Adgang til informationssikkerhedsdokumenter og -registreringer skal gøres tilgængelige for personer med behov for dette.

Informationssikkerhedsdokumenter og -registreringer skal beskyttes på passende måde.

Informationssikkerhedsdokumenter og registreringer skal være underlagt versionsstyring.

8 Drift

8.1 Driftsplanlægning og styring

Operationel planlægning af informationssikkerhed

Næstved Kommune skal lave planer for imødegåelse af identificerede risici

Informationssikkerhedsudvalget skal planlægge, hvordan de aftalte informationssikkerhedsmål opnås, f.eks. ved anvendelse af Årshjul, kontrolkatalog eller lignende.

8.2 Vurdering af informationssikkerhedsrisici

Der gennemføres opfølgning på risikovurderingen mindst en gang om året - eller ved Lovgivningsmæssige, større tekniske eller organisatoriske ændringer - således, at kommunens ledelse kan holdes orienteret om det aktuelle risikobillede.

Resultaterne af risikovurderingen eller opfølgningen heraf skal dokumenteres.

8.3 Håndtering af informationssikkerhedsrisici

Planer for risikohåndtering

På baggrund af risikovurderinger skal der fastlægges planer for imødegåelse af de identificerede risici,

Håndteringen af disse risici skal prioriteres og dokumenteres.

9 Evaluering

9.1 Overvågning, måling, analyse og evaluering

Overvågning af effektiviteten af ISMS'et

Informationssikkerhedskoordinatoren skal kontrollere, at sikkerhedspolitikken er velimplementeret i organisationen og overholdes.
Denne gennemgang skal foretages mindst en gang om året, og gennemgangen skal omfatte beskrivelse af årsagen til afvigelser, handlingsplaner, der er nødvendige for at håndtere afvigelserne (korrigerende handlinger) samt en efterfølgende vurdering af effektiviteten af de foranstaltninger, der gennemføres.

9.2 Intern audit

Revision af sikkerhedspolitik

Der foretages løbende kontrol af, hvorvidt reglerne i Informationssikkerhedshåndbogen samt bilagene i praksis efterleves. Informationssikkerheden kontrolleres og revideres ud fra en konkret vurdering af væsentlighed og risiko.

Informationssikkerhedskoordinator er ansvarlig for at kontrollen iværksættes og at kontrollens resultat afrapporteres til direktion og øverste sikkerhedsansvarlige.

Kontrollen foretages evt. med ekstern bistand.

Med udgangspunkt i information fra Centre, afdelinger og institutioner, har kommunaldirektøren det overordnede ansvar for, at Informationssikkerhedshåndbogen og tilhørende bilag løbende ajourføres. Opgaven er i praksis uddelegeret til Informationssikkerhedskoordinatoren. Ajourføring skal mindst finde sted en gang årligt eller ved større omlægninger i informationsbehandlingen.

Intern informationssikkerheds-audit

Informationssikkerhedskoordinatoren skal vurdere, om Næstved Kommune er i overensstemmelse med Informationssikkerhedspolitikken, Informationssikkerhedshåndbogen og tilhørende bilag.

9.3 Ledelsens gennemgang

Informationssikkerhedskoordinatoren udmønter Informationssikkerhedspolitikken i de fornødne kontroller og informationssikkerhedstiltag. Hvert år aftales plan for kontrol på informationssikkerhedsområdet. Informationssikkerhedskoordinatoren udvælger i samarbejde med Informationssikkerhedsudvalget konkrete fokusområder, og står for den praktiske gennemførelse og afrapportering.

Afrapporteringen fra Informationssikkerhedskoordinatoren skal godkendes i Informationssikkerhedsudvalget

10 Forbedring

10.1 Afvigelser og korrigerende handlinger

Alle Informationsbrugere i kommunen skal være opmærksomme på deres forpligtelser til hurtigst muligt at rapportere informationssikkerhedshændelser til nærmeste leder.
Nærmeste leder skal altid underrette Informationssikkerhedskoordinatoren i sådanne tilfælde. Her vil det blive vurderet, om der er tale om en reel informationssikkerhedshændelse og hvilke foranstaltninger, der skal iværksættes.

Information om afvigelser fra informationssikkerheden

Næstved Kommune skal på faktuel vis informere berørte parter internt og eksternt om eventuelle sikkerhedshændelser. Øverste Informationssikkerhedsansvarlige skal godkende alle eksterne meddelelser.

Opfølgning på afvigelser fra informationssikkerheden

It sikkerhedskoordinatoren er ansvarlig for at indsamle statistik for afvigelser på informationssikkerheden.

Ved konstatering af brud eller formodede brud på informationssikringsforanstaltninger skal der foretages en vurdering

om der er tale om:

- Ineffektive sikringstiltag
- Brud på fortrolighed, integritet og tilgængelighed
- Menneskelige fejl
- Brud på fysisk sikkerhed
- Manglende efterlevelse af politikker eller procedurer
- Brud på logisk adgang
- Malware, virus eller hacking
- Driftsforstyrrelser (systemændringer, hardwarefejl mm.)

10.2 Løbende forbedring

Løbende forbedringer af informationssikkerheden

For at sikre, at ISMS'et til stadighed forbedres, skal Næstved Kommune iværksætte en proces, der gør det muligt for Informationssikkerhedsudvalget at reagere på resultaterne fra overvågning af informationssikkerheden, intern audit og afvigelser.

Udarbejdelse og ikrafttrædelse

Informationssikkerhedspolitikken er udarbejdet af Team servicedesk og IT og kvalitetssikret af Informationssikkerhedsudvalget, der i udarbejdelsesprocessen har fungeret som styregruppe for ISO27001/ISO27002 projektet.

Ændringer i Informationssikkerhedspolitikken besluttes af Økonomiudvalget, mens ændringer i Informationssikkerhedshåndbogen godkendes af direktionen. Ændringer i operationelle procedurer kan foretages i de ansvarlige Centre, afdelinger eller virksomheder.

Informationssikkerhedspolitikken er behandlet på direktionen den

Informationssikkerhedspolitikken er behandlet i Økonomiudvalget den 16.4 2018.

Resultatet af sagsbehandlingen er, at Informationssikkerhedspolitikken er behandlet og endelig politisk godkendt af Byrådet den 24.4 2018.

Underskrift og godkendelse

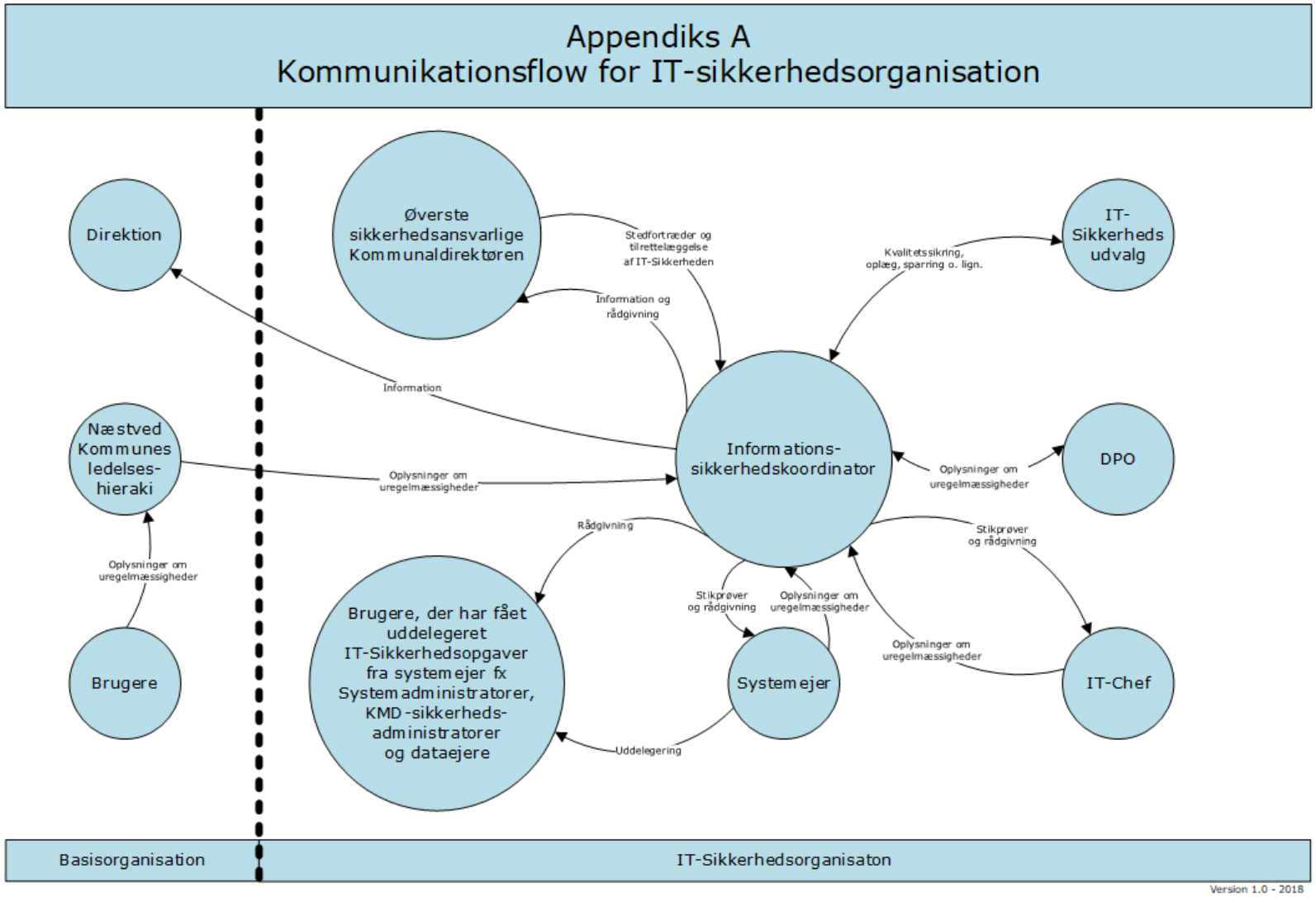
Næstved den 24.4 2018

Borgmester
Carsten Rasmussen

Næstved den 24.4 2018

Kommunaldirektør
Rie Perry

Appendiks A


Appendiks A
Kommunikationsflow for IT-sikkerhedsorganisation
Direktion
Øverste sikkerhedsansvarlige Kommunaldirektøren
IT-Sikkerheds udvalg
Næstved Kommunes ledelses-hieraki
Informations-sikkerhedskoordinator
DPO
Brugere
Brugere, der har fået uddelegeret IT-Sikkerhedsopgaver fra systemejer fx System administratorer, KMD-sikkerheds-administratorer og dataejere
Systemejer
IT-Chef
Stedfortræder og tilrettelæggelse af IT-Sikkerheden
Information og rådgivning
Kvalitetssikring, oplæg, sparring o. lign.
Information
Oplysninger om uregelmæssigheder
Oplysninger om uregelmæssigheder
Oplysninger om uregelmæssigheder
Rådgivning
Stikprøver og rådgivning
Stikprøver og rådgivning
Oplysninger om uregelmæssigheder
Oplysninger om uregelmæssigheder
Uddelegering
Basisorganisation
IT-Sikkerhedsorganisaton
Version 1.0 - 2018