

REFERAT Informationssikkerhedsudvalget d. 14-11-2018

Mødedato Onsdag d. 14. november 2018 kl. 14:00

Mødested Bogense Rådhus, Mødelokale 2

Indholdsfortegnelse

Revision af håndbog for informationssikkerhed.....	3
Living document.....	5
Årshjul for awarenesskampagner for informationssikkerhed.....	6
MDM mobil sikkerhed i design.....	7
Status på databehandler aftaler, KITOS.....	9
Status på implementering af EU-databeskyttelsesforordningen.....	10
Fortegnelser, Datatilsynets tilsyn med kommunerne Informationssikkerhed.....	12

Punkt 1: Revision af håndbog for informationssikkerhed

Sagsfremstilling

1. Revision af håndbog for informationssikkerhed

Åbent

Sagsnr. 480-2018-5834 Dok.nr. 480-2018-249956

Sagens kerne

Informationssikkerhedshåndbogen blev godkendt i direktionen i maj 2018.

Der er pt. tilføjet to nye afsnit;

- Afsnit 16. Persondata på hjemmesiden
- Afsnit 17. Tillidsrepræsentant

Informationssikkerhedsudvalget skal tage stilling til de to tilføjede afsnit og drøfte, om der pt. er behov for yderligere revision/tilføjelser.

Indstilling

At den reviderede informationssikkerhedshåndbog med eventuelle bemærkninger/tilføjelser fra udvalget godkendes.

Sagens baggrund

Informationssikkerhedshåndbogen blev godkendt i direktionen i maj 2018.

Der kommer løbende spørgsmål ind fra medarbejderne omkring arbejdet med informationssikkerhed, hvorfor håndbogen løbende skal revideres, så den altid udgør et så fyldestgørende opslagsværk som muligt.

Der er pt. tilføjet to nye afsnit;

- Afsnit 16. Persondata på hjemmesiden
- Afsnit 17. Tillidsrepræsentant

Informationssikkerhedsudvalget skal tage stilling til de to tilføjede afsnit og drøfte, om der pt. er behov for yderligere revision/tilføjelser.

Økonomiske oplysninger

-

Lovgrundlag

-

Beslutning

Informationssikkerhedsudvalg den 12. oktober 2018

Fraværende: Gitte Clemmensen

Følgende punkter er relevante at tilføje;

- Håndtering af fotos og filmsekvenser fra telefoner, tablets, droner mv. Beskrivelsen udarbejdes af IT-chefen.
- Adgang til kommunale oplysninger på private enheder, fx mail, nexus mv.

Offentliggørelse af en revideret version afventer næste møde i Informationssikkerhedsudvalget.

Revideret version af Informationssikkerhedshåndbogen forelægges.

Bilag

480-2018-146477 Informationssikkerhedshåndbog ver 2.0 kladde

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Se beslutningen på punktet vedr. MDM.

Bilag

Informationssikkerhedshåndbog ver 2.0 kladde

Punkt 2: Living document

Sagsfremstilling

2. Living document

Åbent

Sagsnr. 480-2018-17097 Dok.nr. 480-2018-249957

Sagens kerne

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Indstilling

Til orientering

Sagens baggrund

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2018-249981 Living document 2018 - rev. nov. 2018

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Orientering foretaget.

Bilag

Living document 2018 - rev. nov. 2018

Punkt 4: MDM mobil sikkerhed i design

Sagsfremstilling

4. MDM mobil sikkerhed i design

Åbent

Sagsnr. 480-2018-24354 Dok.nr. 480-2018-255091

Sagens kerne

Sikkerhed og styring af arbejdsrelaterede data og Apps på mobile enheder. (Mail, kalender, billeder, apps mv.)

Indstilling

Forelægges til drøftelse.

Sagens baggrund

Nordfyns Kommunes mobile enheder styres delvist i Mobile Device Management, hvor mail og kalender er beskyttet via sikkerhedsprofil (skærmlås, og wipe mulighed), og hvor apps skubbes ud til enheden (Min kørsel, Børne Intra, Nexus, Drone).

Der er stigende tilgang til mail, kalender, og apps på enheden, som **ikke** har hentet Nordfyns Kommunes sikkerhedsprofil via MDM.

Det kræver ikke så meget teknisk forståelse at sætte dette op.

Ligeledes kan der frit hentes og anvendes apps uden om MDM til alle mulige formål.

Derved ligger arbejdsrelateret data potentielt åben og uden beskyttelse på enheden, som Kommunen ikke kan beskytte på selv et minimumsniveau (fx sikre at skærmlås anvendes).

Datasikkerhed i design (Forordningens Artikel 32) øges på mobile enheder.

MDM løsningen udvides med Secure PIM.

Secure PIM er en ”lukket silo” hvori mail, kalender, billeder, browser er beskyttet af et ekstra lag af sikkerhed (to-faktor kode, wipe mulighed, data isoleret fra misbrug fra andre apps).

Det indstilles til principbeslutning, at MDM Secure PIM og sikkerhedsprofil SKAL være hentet på de enheder, hvorfra man ønsker adgang til, og håndtering af, arbejdsrelaterede data. OGSÅ private enheder (BYOD).

Der lukkes for muligheden for tilgang til mail og kalender på mobile enheder, som ikke har accepteret at underlægge sig kommunens sikkerhedsprofil.

Webmail i browser er alternativet til ovenstående, som beskyttes med 2 faktor login.

Derved har alle stadig mulighed for at tilgå mail på anden vis.

Det indskræpes i Sikkerhedshåndbogen at Apps skal cleares af It-afdelingen, og skubbes ud til enheden via MDM, for at sikre data med central styring (sletning af data, koder, trække app'en tilbage fra enheden).

Apps som hentes og anvendes udenom MDM løsningen har IKKE kommunens accept, hvorfor al risiko, sikkerhedsbrud på data og påtaler (bødeforlæg) falder tilbage på afdelingens leder.

Sikkerhed i Design øger driftsudgifter, som derfor må indregnes på forkant ved fremtidige indkøb af diverse systemer / services.

Økonomien bør dækkes decentralt for afdelingens egne løsninger, og centralt for Koncernens bredt dækkende løsninger.

Økonomiske oplysninger

MDM og Secure PIM er licensbaseret, og betales decentralt af afdelingen som ejer enheden. For de enheder, der er aftale med fra It-afdelingen inkluderes dette i det månedlige service gebyr pr. enhed, hvor prisen stiger fra den nuværende pris kr. 200 kr. til kr. 250 om måneden.

For alle enheder, der ikke er ejet af Nordfyns Kommune, der ønsker at tilgå mail og kalender, lægges en Secure PIM på enheden til en pris af kr. 50 pr. måned. Denne aftale skal indgås med den enkeltes afdeling og betales af afdelingen.

Lovgrundlag

Intet.

Bilag

480-2018-255236

Secure Pim introduktion

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Informationssikkerhedsudvalget godkender følgende:

- det er konstateret, at der er risiko for at medarbejdere kan tilgå mail og kalender via apps på deres private enheder udenom Nordfyns Kommunes valgte sikkerhedsprofiler. Denne mulighed lukkes.

Informationsudvalget anbefaler direktionen, at sikkerheden skærpes på kommunens egne enheder, så arbejdsrelaterede data isoleres via PIM. Forslaget forelægges direktionen til godkendelse, når der er udarbejdet en mere detaljeret analyse af de økonomiske konsekvenser, og der ligger et forslag til udrulningsplan.

Bilag

Secure Pim introduktion

Punkt 5: Status på databehandler aftaler, KITOS

Sagsfremstilling

5. Status på databehandler aftaler, KITOS

Åbent

Sagsnr. 480-2018-24379 Dok.nr. 480-2018-255336

Sagens kerne

Registreringerne i KITOS gennemgås med henblik på at sikre, at arbejdet med databehandleraftaler og opdateringen af KITOS er i fortsat fremdrift.

Indstilling

Det indstilles, at Informationssikkerhedsudvalget gennemgår registreringerne i KITOS for så vidt angår registrering af databehandleraftaler og system- og dataansvarlige.

Sagens baggrund

Nordfyns Kommune har udarbejdet en procedure for indgåelse af databehandleraftaler. Hvorvidt der er indgået databehandleraftaler fremgår i KITOS, som er kommunens oversigt over kommunens systemer.

Af KITOS fremgår også, hvem der er system- og dataansvarlig. Det fremgår af informationssikkerhedsorganisationen, at den system- og dataansvarlige er en niveau 2 eller 3 chef/leder.

Ansvar for registreringen i KITOS ligger, jf. informationssikkerhedsorganisationen, i IT-afdelingen.

På mødet gennemgås registreringerne i KITOS med henblik på at sikre, at arbejdet med databehandleraftaler og opdateringen af KITOS er i fortsat fremdrift.

Der henvises til intranettet;

<https://intranet.nordfynskommune.dk/Om-kommunen/Informationssikkerhed/Databehandleraftale>

For yderligere inspiration til punktet er vedlagt en udgave af IT-magasinet KIT, som netop berører temaet vedr. databehandleraftaler.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2018-255534

kitmagasinet_20180830

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Genbehandles med opdateret data.

Bilag

kitmagasinet_20180830

Punkt 6: Status på implementering af EU-databeskyttelsesforordningen

Sagsfremstilling

6. Status på implementering af EU-databeskyttelsesforordningen Åbent

Sagsnr. 480-2017-34778 Dok.nr. 480-2018-255400

Sagens kerne

Opfølgning og afslutning af de resterende opgaver i kommunens 12-punktsplan vedrørende implementering af EU-databeskyttelsesforordningen.

Indstilling

Det indstilles, at nævnte opgaver godkendes som afsluttede.

Sagens baggrund

Informationssikkerhedsudvalget drøftede på mødet den 12. oktober 2018 en status på implementering af EU-databeskyttelsesforordningen, hvor der arbejdes efter vedlagte 12-punktsplan.

En række af punkterne blev afsluttet på mødet den 12. november 2018. De med rødt markerede opgaver er opgaver, som endnu ikke er afsluttede. Det drejer sig om følgende;

Opgave 8:

Der skal udarbejdes en procedure for sikkerhedsbrud, herunder skal der udarbejdes blanket. Procedure og anmeldelsesblanket skal lægges på Intranettet.

Ansvar: DPO.

Afsluttet: Uge 43.

Opgave 11:

Nordfyns Kommune er som offentlig myndighed ikke omfattet af personers rettighed til at blive glemt. Det skal undersøges, om Justitsministeriets vejledning for medarbejderne er blevet udgivet.

Ansvar: DPO.

Afsluttet: Afklares til næste møde.

Opgave 12:

Af bilaget fremgår, at det generelt kan oplyses, at der for de fleste af nye tiltag (konsekvensanalyser og databeskyttelse gennem design og standardindstillinger) ikke skal laves bagudrettet for de løsninger, der er kørende i drift i dag. Men det er vigtigt, at konsekvensanalyserne indarbejdes i processen for udbud og kontraktindgåelse ved køb af nye systemer, som konsekvensanalysen er udarbejdet, når der indgås aftale og underskrives databehandleraftale.

Selvom det som udgangspunkt ikke skal gælde bagudrettet, så skal systemer screenes med henblik på at afsøge, om der er systemer der bør udarbejdes konsekvensanalyse for. Her skal fokus være rettet mod systemer, som fx alene kører på decentrale institutioner, er indkøbt decentral og som behandler persondata.

Ansvar: DPO.

Afsluttet: Til næste møde i Informationssikkerhedsudvalget er systemerne screenet med henblik på en indstilling til Informationssikkerhedsudvalget om hvilke eksisterende systemer, som der bør udarbejdes konsekvensanalyse for.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2018-255384 Status på implementering af EU-databeskyttelsesforordningen november

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Indstillingen godkendt.

Bilag

Status på implementering af EU-databeskyttelsesforordningen november

Punkt 7: Fortegnelser, Datatilsynets tilsyn med kommunerne Informationssikkerhed

Sagsfremstilling

7. Fortegnelser, Datatilsynets tilsyn med kommunerne Informationssikkerhed Åbent

Sagsnr. 480-2018-22032 Dok.nr. 480-2018-255432

Sagens kerne

Status på standardfortegnelser.

Indstilling

Til orientering.

Sagens baggrund

På mødet i Informationssikkerhedsudvalget drøftede udvalget Datatilsynets udmelding på temaer til de kommende tilsyn ved kommunerne i 2018.

Èt af temaerne er ”udarbejdelse af fortegnelser”. Udvalget besluttede, at Nordfyns Kommune tiltræder standardfortegnelserne.

Udvalget besluttede videre denne proces;

1. DPO fremsender standardfortegnelsen til de relevante dataansvarlige (KITOR).
2. De dataansvarlige tager stilling til, om fortegnelserne stemmer med de faktiske forhold og arbejder med persondata.
3. Den dataansvarlige kvitterer tilbage med eventuelle bemærkninger/rettelser.
4. DPO lægger kvitteringen på en samlet sag, som vedrører fortegnelserne. Oplysningen registreres i KITOS.

DPO giver en status på arbejdet siden sidst.

Økonomiske oplysninger

-

Lovgrundlag

-

Beslutning

Informationssikkerhedsudvalg den 14. november 2018

Fraværende: Ingen

Følger den proces som blev aftalt sidst.