IT-sikkerhedspolitik for Lyngby Tandplejecenter

1 Indledning

Formål med IT-sikkerhedspolitikken
Lyngby tandplejecenters IT-sikkerhedspolitik er vores sikkerhedsgrundlag og vores fælles forståelse af, hvad IT-sikkerhed er. IT-sikkerhedsstrategien og IT-sikkerhedspolitikken fastlægger vores ambitionsniveau og opstiller rammerne for de sikkerhedstiltag, som er nødvendige at følge, når vi som klinik skal leve op til lovgivningskrav og best practices.

Lyngby tandplejecenter ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement i forhold til at kunne tilbyde en sikker service over for patienter, myndigheder og samarbejdspartnere i det hele taget.

Med IT-sikkerhed forstår vi den nødvendige beskyttelse af samtlige ressourcer, der indgår i - eller bidrager til Lyngby Tandplejecenters behandling og kommunikation af data elektronisk eller i papirform mv.

Hovedmålsætninger i IT-sikkerhedspolitikken

IT-sikkerhed og troværdighed
IT-sikkerheden skal understøtte Lyngby tandplejecenters virksomhed i forhold til at sikre stabilitet i tilgangen til data, fortrolighed i forhold til personfølsomme data samt pålidelighed i datas indhold. Dette sikres ved, at Lyngby tandplejecenter i vores dagligdag lever op til almindelige principper for IT-sikkerhed.

Lyngby Tandplejecenter benytter it i forb.m.bl.a. :

- Patientbehandling
- Samarbejde med myndigheder og forsikringsselskaber
- Administration
- Behandling af patient- og personaledata

Målet for IT-sikkerheden er at:

- Understøtte bevidstheden om IT-sikkerhed i klinikken
- Opnå høj driftssikkerhed og minimeret risiko for store nedbrud og tab af data
- Opnå mulighed for fortrolig behandling, transmission og opbevaring af data. Dvs. at faciliteter hertil skal være til stede og benyttes efter konkret behov
- Sikre mod forsøg på brud på sikkerhedsforanstaltninger

Afbalanceret IT-sikkerhed
Lyngby tandplejecenter er afhængig af et godt omdømme og tillid fra patienter og samarbejdspartnere. Derfor skal IT-sikkerhedspolitikken være med til at sikre, at data og informationer behandles i overensstemmelse med gældende lovkrav. Sikkerhedsniveauet skal dog afbalanceres, således at fleksibiliteten og dynamikken i vores dagligdag ikke mistes. Derfor er det en målsætning i sikkerhedspolitikken, at data og systemer sikres ud fra en vurdering af, hvad der er nødvendigt at gøre under hensyntagen til de økonomiske rammer.

Omfang
IT-sikkerhedspolitikken er det dokument, der angiver de beslutninger, som ledelsen i Lyngby Tandplejecenter har truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der skal stilles, for at sikkerhedsniveauet opretholdes.

Derfor fastlægges omfanget af IT-sikkerhedspolitikken således:

- IT-sikkerhedspolitikken gælder for alle ansatte i Lyngby Tandplejecenter uanset ansættelsesform, herunder også eksterne konsulenter. Det forventes, at IT-sikkerhedspolitikken overholdes.
- IT-sikkerhedspolitikken gælder for alle systemer og alle data i Lyngby Tandplejecenters besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til klinikkens systemer og data, skal ligeledes have kendskab til og følge IT-sikkerhedspolitikken.
- IT-sikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Lyngby tandplejecenters it-systemer og papirarkiver.
- IT-sikkerhedspolitikken godkendes af ledelsen og revurderes en gang årligt for at sikre, at den stadig er i overensstemmelse med virkeligheden.

2 Risikovurdering og risikoanalyse

Risikovurdering
Det sikkerhedsniveau, denne politik repræsenterer, er fastsat på baggrund af Lyngby Tandplejecenters vurdering af de forretningsmæssige it-risici, som vi ønsker at imødegå.

It-risikovurderingen opdateres ved eventuelle større ændringer i it-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer med efterfølgende tilretning af informations-sikkerhedspolitikken, retningslinjer mm.

Sikkerhedsniveau
Lyngby Tandplejecenters sikkerhedsniveau skal først og fremmest indfri de forventninger til troværdighed og stabilitet, der er til behandling af forretningskritiske data på en tandklinik. Lyngby tandplejecenter ønsker at fremstå med et højt sikkerhedsniveau, der tilgodeser:

- Lovgivning
- Anerkendt best practice inden for IT-sikkerhed

3 Organisering og ansvar

Interne organisatoriske forhold
Organisering af IT-sikkerhed er som følger:

Ledelsen sørger løbende for at it-sikkerheden overholdes samt at samarbejdspartnere overholder deres forpligtelser.

Processerne er beskrevet i interne instrukser.

Styringsprincipper
IT-sikkerhed er et fælles anliggende for hele klinikken. Håndteringen af IT-sikkerhed vil blive ledet af ledelsen.

Eksterne samarbejdspartnere
Hvis en ekstern samarbejdspartner gives adgang til eller hvis disse behandler data på vegne af Lyngby tandplejecenter, skal der indgås skriftlige databehandlingsaftaler med eventuelle eksterne samarbejdspartnere om dette.

4 Klassifikation af systemer og data
For at sikre at vores systemer og data har det rigtige sikkerhedsniveau, skal disse identificeres og klassificeres løbende.

5 Brugeradfærd
Opretholdelse af det ønskede sikkerhedsniveau er afhængig af, at vi alle tager ansvar for informationssikkerheden.

Alle ansatte er bekendt med sikkerhedspolitikken og gældende retningslinjer for ønsket adfærd.

Anvendelse af it og behandling af data er almindelige redskaber i varetagelsen af de daglige arbejdsopgaver. Håndteringen af patientdata kræver faglige forudsætninger, og bør desuden ske med omtanke og almindelig sund fornuft.

Det er vigtigt, at følge disse retningslinjer:

- Persondata behandles i alle tilfælde fortroligt.
- Der anvendes login og password, og password skiftes med jævne mellemrum.
- Datamedier med persondata og vigtige informationer behandles og beskyttes med omhu mod at uvedkommende får adgang til dem.
- Det er vigtigt at kunne anvende internettet i mange sammenhænge. Dog er besøg på sider med racistisk, uetisk eller pornografisk indhold ikke acceptabelt i forbindelse med de daglige arbejdsopgaver.
- Mail anvendes til kommunikation af kliniske eller forretningsmæssige formål. Privat korrespondance er ikke tilladt.
- Der må kun anvendes it-programmer, som er godkendt af ledelsen.
- Hvis man oplever, at der sker brud på IT-sikkerheden, er det vigtigt at informere ledelsen – benyt Lyngby tandplejecenters it-beredskabsplan.

Passwordsikkerhed
For at sikre klinikkens data skal der benyttes passwords.

Ansættelsesforholdet
Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau i Lyngby tandplejecenter. For at kunne leve op til medansvaret, er det den Virksomhedsansvarlige, Margit Andersen's ansvar at sørge for instruktion i forhold til anvendelse af systemer i det daglige arbejde samt i forhold til den ønskede adfærd for IT-sikkerhed. Alle medarbejdere skal:

- Have et generelt kendskab til IT-sikkerhed
- Kende deres ansvar for sikkerheden
- Sikre deres personlige adgangskoder, samt personligt udleverede systemadgangskoder.
- Passe på it-udstyr
- Deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden
- Rapportere hændelser, der kan indikere brud på sikkerheden

Som afhjælpningsforanstaltninger til at minimere vurderede risici, skal retningslinjerne revurderes og opdateres årligt eller ved større forandringer. Overtrædelser af IT-sikkerhedspolitikken vil efter omstændighederne kunne medføre ansættelsesmæssige sanktioner.

Funktionsadskillelse
Der er etableret egentlig funktionsadskillelse, hvor det er nødvendigt. Det betyder, at ved installering af programmel, vurderes det i forbindelse med oprettelse af medarbejder, hvilke programmer vedkommende medarbejder skal have adgang til.

Ansættelsens ophør
Der er procedurer, der sikrer, at it-aktiver returneres, og at adgange og rettigheder ophører ved ansættelsesforholdets ophør. Nøgler afleveres, personlige brugerkonti de-aktiveres, og fælles systempasswords skiftes.

6 Fysisk sikkerhed
Adgangen til alle fysiske lokaliteter er sikret mod uvedkommendes adgang.

Sikre områder
Lyngby tandplejecenter er aflåst udenfor klinikkens åbningstider og der er etableret alarmsystem til externt alarmfirma.

Fysisk adgangskontrol
Adgang til Lyngby Tandplejecenter udenfor åbningstid tildeles ved udlevering af nøgler som gæstenøgle til fx håndværkere. Alle it-data vil i disse tidsrum være slukkede.

Beskyttelse af udstyr
It-udstyr er ikke i særlig grad beskyttet mod ødelæggelse og skade, der følger af brand, vandskade, strømsvigt og andre skader, som udspringer af hændelser i det omkringliggende miljø. Back-up foretages af ekstern samarbejdspartner, som Lyngby tandplejecenter har outsourcet it til.

Ved bortskaffelse, reparation eller genbrug af it-udstyr sikres det, at udstyret er forsvarligt renset for alle data.

7 Styring af netværk og drift
Foretages af It-Foqus som extern it-samarbejdspartner.

Eksterne serviceleverandører
I aftaler med de eksterne serviceleverandører skal det fremgå, at disse skal varetage kontroller, som udføres på vegne af Lyngby Tandplejecenter hensigtsmæssigt og i overensstemmelse med det aftalte.

Skadevoldende programmer (vira, orme, spy- og malware)
Skadevoldende programmer kan sætte hele klinikken ud af drift, og det kan være meget dyrt at rense it- systemerne, hvis de er blevet ramt af ransomware, virus eller et hackerangreb.

Alt godkendt it-udstyr, der er tilsluttet Lyngby tandplejecenters netværk har installeret et aktivt og opdateret antivirusprogrammel, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer. Det gælder også eksterne brugere, der tilsluttes netværket via fjernopkobling. Det overvåges, at antivirusprogrammerne hele tiden er opdaterede.

Det er ikke tilladt at installere egne programmer på Lyngby tandplejecenters maskiner. Det er kun administrator der har rettigheder til at installerede programmer.

Netværkssikkerhed
For at undgå uautoriseret adgang, er vores netværk sikret.

Informationsudveksling

Regler i forbindelse med informationsudveksling af fortrolig information sker via sikker e-mail, journalprogram.

8 Adgangsstyring

De forretningsmæssige krav til adgangsstyring
Alle informationsaktiver (papir sager, elektroniske sager, programmel, udstyr, data, informationer og databærende medier) skal i nærmere specificeret omfang være beskyttet mod uautoriseret adgang.

Ud over den nødvendige adgangskontrol til bygninger og lokaler, anvendes der elektroniske/-programmel- baserede adgangskontrolsystemer.

Administration af brugeradgang
Tildeling, ændring og sletning af brugeradgang til systemer og data sker ud fra arbejdsbetingede behov i overensstemmelse med datas klassifikation. Fysiske adgange og brugerrettigheder til netværk og systemer inddrages, når brugeren ikke længere skal have adgang.

Brugerens ansvar
Alle medarbejdere er ansvarlige for at holde de udleverede adgangskoder hemmelige.

Mobilt udstyr og fjernarbejdspladser
IT-sikkerhedspolitikken gælder for alt it-udstyr tilhørende Lyngby Tandplejecenter. I IT-sikkerhedshåndbogen for medarbejdere fastlægges de regler, som skal overholdes ved evt. brug af

mobilt udstyr og hjemmearbejdspladser.

9 Anskaffelse, udvikling og vedligeholdelse af it-systemer

Sikkerhedskrav til informationsbehandlingssystemer
De sikkerhedskrav, der stilles til systemers behandling af data, skal indgå i vurderingen, som foretages ved indkøb af nye systemer. Ved indkøb af nye it-systemer skal analyse af behandling af persondata og sikkerhed vurderes.

Kryptering
Behovet for brug af kryptering skal identificeres ud fra en vurdering af, hvor kryptering som sikringsforanstaltning kan imødekomme behovet for sikring af datas fortrolighed og/eller integritet. Det sker på grundlag af datas klassifikation.

It-beredskabsstyring
Lyngby Tandplejecenter har udarbejdet en it-beredskabsplan med en praktisk strategi for, hvordan Lyngby tandplejecenter organisatorisk skal håndtere en beredskabssituation. Beredskabets arbejde består i at begrænse konsekvenserne af tab af data og systemer forårsaget af sikkerhedsbrister.

Der henvises i øvrigt til Lyngby tandplejecenters beredskabsplan.

10 Overensstemmelse med lovbestemte krav
Da der er flere lovgivninger, der påvirker vores daglige administration, skal der tages højde for disse i vores IT-sikkerhedspolitik og de dertilhørende retningslinjer. Lyngby Tandplejecenters retningslinjer og procedurer skal være i overensstemmelse med alle sikkerhedskrav i lovgivning og med indgåede kontrakter.

11 Godkendelse

IT-sikkerhedspolitikken er godkendt af Virksomhedsansvarlig tandlæge, Margit Andersen

Dato: 0105-2018
_____-_____
Underskrift:

_____