

Datasikkerhed og –fortrolighed

STANDARD	Datasikkerhed og –fortrolighed
FORMÅL	<i>At sikre beskyttelse mod misbrug af personfølsomme data. Fortrolighed, tilgængelighed samt hensigtsmæssig og kontrolleret adgang for relevant brug af data i overensstemmelse med gældende lovgivning.</i>
ANVENDELSESOMRÅDE	<i>Medarbejdere i Tandplejen Randers.</i>

RETNINGSLINIE

TRIN 1	• <i>Der eksisterer i Randers kommune en IT-sikkerhedspolitik, en tilknyttet it-sikkerhedsportal og -håndbog som erstatter denne vejledning i datasikkerhed og fortrolighed.</i> • <i>For ved systemnedbrud og support af IT kontaktes support-afdelingen på telefon 89 15 18 18, mail: itsupport@randers.dk</i> • <i>Ansaret for hvad der foregår på PC fra der logges på til der logges af, ligger hos den enkelte medarbejder.</i> • <i>Adgangskoden er personlig og må ikke udleveres til andre. Ved behov kan den udleveres til en it-medarbejder.</i> • <i>Persondata herunder patientjournaler og røntgenbilleder opbevares på en central server. Der bliver løbende taget sikkerhedskopier af server med TK2 og Digora samt af F drevet og den enkeltes personlige drev.</i> • <i>Der bliver ikke taget sikkerhedskopier af løse drev som CD-rom og USB-drev.</i> • <i>Når arbejdspladsen forlades i løbet af arbejdsdagen skal PC'eren sikres mod uautoriseret adgang ved at den låses med pauseskærm sikret med adgangskode.</i> • <i>Ved arbejdsophør lukkes PC helt ned.</i>
--------	--

- *Der er følgende krav til adgangskoderne :*
- *Adgangskoden skal skiftes hver 3. måned.*
- *Koden skal være på minimum 8 tegn og en blanding af bogstaver og tal.*
- *Adgangskoden kan ikke genbruges.*
- *Hvis der opdages trusler mod it-driftsafviklingen, forsøg på uautoriseret adgang eller overtrædelser af it-sikkerhedsreglerne, skal kommunens it-sikkerhedsleder eller nærmeste leder underrettes.*
- *Antivirusprogrammet eller fire-wall'en må ikke afbrydes.*
- *Programmer må ikke installeres uden at superbrugers eller it-afdelingens godkendelse.*
- *Hvis der er mistanke om virus skal computeren straks slukkes og it-afdelingen underrettes.*
- *Ved udskrivning af dokumenter skal det sikres at oplysningerne ikke bliver tilgængelige for uvedkommende. Ved udskrivning på fælles printere skal dokumenterne straks hentes.*
- *Papir med fortrolige data skal makuleres efter brug.*
- *Fortrolig information eller personhenførbare oplysninger skal altid sendes som sikker e-mail.*
- *De ansatte har tavshedspligt og skal overholde persondataloven.*
- *Ved annoncerede systemlukninger udskrives arbejdsopgaverne på papir, journalen føres i hånden og indskrives elektronisk snarest muligt efter opstart af systemet.*
- *Ved akut systemnedbrud aflyses behandlingerne for de patienter, hvor behandlingen ikke kan gennemføres på*

	<i>forsvarlig vis.</i>
TRIN 2	Medarbejderne ved tandplejen kender og anvender retningslinjen.
TRIN 3	Der foretages årlig overvågning af, om medarbejderne anvender forholdsreglerne.
TRIN 4	På baggrund af kvalitetsovervågningen prioriterer ledelsen iværksættelse af konkrete tiltag for kvalitetsforbedringer jf. Standard Kvalitetsforbedringer.

Tidsramme for revision :

Dette dokument er gyldigt i en 3 årig periode fra 2023 - 2025

Ansvarsplacering :

Lederen af tandplejen har ansvaret for retningslinjens indhold og for at medarbejderne kender og anvender den.

Lederen af tandplejen har ansvar for, at den årlige overvågning finder sted.