



Sikkerhed
I BIRKERØD KOMMUNE



Indhold

4

Regler & retningslinier for IT-brugere i Birkerød Kommune

6

Om computervirus og hvordan det kan undgås

8

Regler & retningslinier for e-post (elektronisk post)

10

Regler & retningslinier for internet

12

Regler & retningslinier for brugerrettigheder

Sikker IT

i Birkerød Kommune

Denne folder har til formål at sætte fokus på IT-sikkerheden i Birkerød Kommune.

Den indeholder fire afsnit om regler og retningslinier for IT-brugere, håndtering af e-post, internet og brugerrettigheder. Det er områder, som er vigtige at være opmærksom på i det daglige arbejde for alle IT-brugere i Birkerød Kommune.

Det er Birkerød Kommunes målsætning at ansatte, der anvender kommunens IT-systemer, skal være i stand til at løse deres arbejdsopgaver effektivt og optimalt. Derfor er der mange gode grunde til, at du giver IT-sikkerhed lidt opmærksomhed i løbet af din

arbejdsdag, både for din egen og dine kollegers skyld.

Der er et gammelt ordsprog, som siger, at ingen kæde er stærkere end det svageste led. Det gælder også for IT-sikkerhed.

Vigtigheden af IT-sikkerhed, eller rettere sagt mangel på samme, bliver du typisk først opmærksom på, når skaden ER sket og det ER for sent. Som for eksempel når computeren strejker! Og du kan ikke komme videre med arbejdsopgaverne.

Måske har du været i situationen før? Og måske kan du stadig huske følelsen af at miste vigtige dokumenter, eller computeren,

der går ned, når du har mest travlt? Men det behøver faktisk ikke at komme så vidt. For med en smule omtanke kan du spare dig selv for mange kvaler og spildt arbejdstid.

Den bedste måde du beskytter din computer og dokumenter på, er ved at bruge din sunde fornuft og huske på folderens regler, retningslinier og gode råd.

Derfor kan du med fordel lægge denne folder ved computeren.

Måske er hjælpen lige ved hånden, næste gang du har brug for et godt IT-råd. Og husk, at du også er velkommen til at kontakte IT-organisationen.



Regler & retningslinier

Tænk IT-sikkerhed – også for din egen skyld

Som bruger af kommunens netværk er du ansvarlig for de aktiviteter, der sker på din computer, lige fra du logger ind, til du logger ud. Forlades computeren ulåst, har andre adgang, og dermed øges risikoen for misbrug.

Står din computer et offentligt sted, er risikoen for, at uvedkommende får adgang til computeren stor. Befinder den sig på et kontor, hvor du og dine kolleger normalt kun kommer, er risikoen mindre.

Uanset hvad, er det altid fornuftigt at logge ud/låse computeren, når du forlader den. Det kan du læse mere om på den næste side.

Find på en god adgangskode

Som ansat har du adgang til systemer, der indeholder fortrolige og personfølsomme data.

Derfor skal din adgangskode udskiftes hver 90. dag. Får du mistanke om, at andre har fået kendskab til koden, skal den udskiftes omgående. I værste fald kan du blive holdt ansvarlig for andres ulovlige handlinger.

En god adgangskode skal være vanskelig at gætte for andre. Koden **skal** være på mindst otte karakterer og indeholde mindst ét bogstav og ét tal.

Koden kan være en blanding af store og små bogstaver.

Anvend aldrig dit eget navn, egne eller nærmeste families initialer, fødselsdag, bilnummer, hundenavn eller lignende, da det er oplagt for uvedkommende at afprøve netop denne type af kombinationer.

Undgå specialtegn som # € / @ og bogstaverne Æ æ Ø ø Å å,

da specielle danske bogstaver kan give systemmæssige problemer. Benyt derfor kun tal, samt de 25 første bogstaver i alfabetet.

Hvis du får kendskab til forsøg på eller ulovlig adgang til kommunens IT-systemer, har du pligt til at underrette IT-organisationen omgående.

Regler for anvendelse af programmer og licenser

Du må ikke installere og anvende andre programmer på Birkerød Kommunes computere/netværk, end dem som kommunen har programlicens til.

Hvis du har behov for andre programmer og applikationer, kan installation finde sted efter aftale med IT-organisationen.

Alle computere, uanset om de er opkoblet som stationære eller bærbare computere, betragtes

som værende en del af Birkerød Kommunes netværk.

Det betyder, at bærbare computere er underlagt de samme regler for programanvendelse og programlicenser som stationære computere.

Sådan låser du computeren

På en Rådhuscomputer:

Tryk på tasterne, **Ctrl – Alt – Delete**

Tryk på knappen: "Lås computeren".

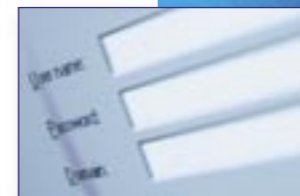
Computeren er nu låst.

På en Citrixxklient:

Tryk på tasterne, **Ctrl – F1**

Tryk på knappen: "Lås computeren".

Computeren er nu låst.



"At forlade en computer ulåst svarer til at forlade bopælen med nøglen i dørlåsen"

"Vis aldrig din adgangskode til nogen. Du giver jo heller ikke din hoveddørsnøgle ud til andre mennesker"



hvordan kan det undgås?

Computervirus

Computervirus er en samlet betegnelse for programstumper, der kan skade din og andres computere. En virus kan kopiere og sprede sig selv til andre computere gennem netværk, og det kan gå hurtigt.

Virus er en alvorlig trussel, fordi den kan ødelægge og slette dine dokumenter på harddisken og sætte ét eller flere vitale netværk ud af drift. De mest kendte former for vira er orme, trojanske heste, makrovirus og hoax.

Tjek på antivirusprogrammet

For at undgå vira har Birkerød Kommune installeret antivirusprogram på alle computere, der opdateres regelmæssigt, så eventuelle nye vira opdages og fjernes. Alligevel kan en virus på flere måder overføres til din computer. Det kan ske gennem internet og e-post, som ofte er årsag til langt

størstedelen af virusangreb. Disketter, CD-ROM og lagringsmedier gennem en USB port kan også være årsag til et virusangreb. Derfor skal du altid bruge din sunde fornuft, når du arbejder på internettet, modtager eller sender e-post og være varsom med at tilslutte eksterne medier til computeren.

Minimér risikoen for virus

Du må aldrig hente filer eller programmer fra internettet, med mindre andet er aftalt med den IT-ansvarlige/IT-organisationen. Du må heller ikke installere andre programmer på kommunens computere end dem, som er indkøbt på legal vis til formålet.

Vær kritisk, når du modtager e-post med en vedhæftet fil. Du kan for eksempel stille dig selv følgende spørgsmål: Har jeg bedt om at få filen tilsendt? Kender jeg afsenderen? Er det sandsynligt, at

afsenderen ville sende e-post med en vedhæftet fil?

Anvendelse af lagringsmedier

Der må ikke være tilsluttet lagringsmedier til din computer, når den tændes og overfører aldrig data fra lagringsmedier til computeren, hvis du ikke kender oprindelsen.

Anvend altid kommunens anti-virusprogram på disketter, der har været uden for huset, eller på anden måde været i kontakt med eksterne computere. Hvis anti-virusprogrammet ikke finder noget mistænkeligt, bør din computer være i orden.

Ved mistanke om virus

Har computeren fået virus, skal du slukke for den og kontakte IT-organisationen. Overvej hvordan virus kan være kommet ind, så fremtidige virusangreb kan forebygges.

“Ved korrekt dokumentdeling og drevanvendelse bevares dine dokumenter for fremtiden”.

Kommunens centrale servere fungerer som store netværkscomputere, hvor du og andre brugere kan hente, gemme og dele data på en række fælles serverdrev.

Som IT-bruger skal du altid gemme filer og dokumenter på det fælles afdelingsdrev N:\, fordi der tages sikkerhedskopi, i modsætning til din computers harddisk, hvor der ikke tages nogen sikkerhedskopi.

På din computer hænger opdelingen af drevene sammen med dens opbygning, herunder harddisken, kaldet C:\ drevet og diskettedrevet, kaldet A:\ drevet.

Skemaet til højre skitserer de forskellige drev, som du har adgang til i Birkerød Kommune.

Drev:	Anvendelsesområde:
A:\	Dit eget diskettedrev.
C:\	Ej tilgængelig.
E:\	Ej tilgængelig.
H:\	Arbejdsrelateret data gemmes i folderen "Kommune". Private data kan i begrænset omfang gemmes i folderen "Privat".
N:\	Afdelingsdrev, placeret på netværket og kan kun anvendes af din afdeling/område.
R:\	Fællesdrev på netværket, hvor diverse filer placeres og deles af flere brugere.
S:\	Programdrev, placeret på netværket, hvor hovedparten af Birkerød Kommunes fagprogrammer er installeret.

Regler & retningslinier for **E-post** *(elektronisk post)*

Regler og retningslinier for indgående e-post

Du har pligt til at kontrollere din personlige postkasse dagligt.

Din e-postkasse kan i begrænset omfang anvendes til at modtage privat e-post.

Regler og retningslinier for udgående e-post

E-post er bedst til korte meddelelser. Lange meddelelser bør du sende som vedhæftede dokumenter.

Anvend "svar med historik", med mindre den oprindelige e-post er meget lang. Det vil hjælpe modtageren, at der refereres til den oprindelige e-post.

Du skal oprette en fast signatur til at sætte under din e-post med minimum navn på afsender, navn på arbejdsplads/område, telefon-

nummer, e-postadresse til arbejdsplads/område og personlig e-postkasse.

Udgående e-post skal sendes til én så præcis målgruppe som muligt. Anvend derfor private distributionslister, hvis de officielle postlister rammer for bredt.

E-post, der anvendes i forbindelse med sagsbehandling, skal holdes i samme sprog som papirbaseret kommunikation. Generelt for e-post gælder, at formuleringen og tonen skal kunne tåle offentliggørelse.

Oplysninger, der sendes med e-post, skal være i overensstemmelse med god etik og sund fornuft, og må ikke være af nedsættende eller diskriminerende art eller have et umoralsk indhold.

For anvendelse af e-post til fortrolige samt personfølsomme

oplysninger henvises der til den uddybende udgave af "IT Sikkerhedspolitik i Birkerød Kommune".

Læs mere i personalehåndbogen for uddybende information.

Overvågning af e-post

Får Birkerød Kommunes IT-ansvarlige mistanke om misbrug af kommunens IT-systemer, kan din indgående og udgående e-post overvåges, uden at du eller andre nødvendigvis informeres om det.

Såfremt overvågning finder sted, vil det ske ud fra en hensyntagen til drift, sikkerhed og genetablering af kommunens IT-systemer, og kun hvis kommunaldirektøren på forhånd har givet tilladelse.

Hvilke oplysninger registreres?

Der registreres kun oplysninger af teknisk karakter omkring den indgående og udgående e-post.

Det vil sige informationer om, hvilke servere posten har passeret, hvem afsender og modtager er, hvornår den er afsendt, og eventuelt hvad emnefeltet er.

Der registreres IKKE for indhold. Ovennævnte informationer opbevares for én måned ad gangen, til for eksempel fejfinding og eftersporing af e-post.



Regler & retningslinier for **Internet**

Arbejd sikkert på Internettet

Internettet indeholder store informationsmængder, og sikker internetbrug kræver din omtanke og sunde fornuft.

I Birkerød Kommune er du velkommen til at anvende "World Wide Web", også forkortet WWW, til arbejdsmæssige formål. Du må også gerne anvende internettet til private formål uden for arbejdstiden. Det vil sige, når arbejdsdagen er afsluttet eller du er flekset ud.

Når du er på internettet, skal du overholde samme regler og fornuftsmæssige overvejelser, som når du anvender kommunens IT-systemer.

Generelt skal du altid handle ud fra almindelig sund fornuft og god IT-skik, og du må under ingen omstændigheder foretage

programmelle ændringer, som for eksempel i Internet Explorer, fordi det kan forringe computerens sikkerhedsindstillinger og dermed åbne op for virus.

På med net-etiketten

Når du surfer rundt på internettet, skal du være opmærksom på at opretholde en "net-etikette", idet du er repræsentant for Birkerød Kommune.

Birkerød Kommune har ikke opstillet faste og evigt gyldige regler for en net-etikette, men opfordrer alle medarbejdere til at være opmærksom på følgende retningslinier:

Ved besøg på hjemmesider efterlader din computer ofte et elektronisk fingeraftryk, så modtageren kan se, hvor din computer kommer fra. Du skal derfor afholde dig fra at besøge hjem-

mesider af mindre lødig karakter. Eksempelvis er besøg på hjemmesider for pædofili mv. ulovlig i medfør af anden lovgivning. Undlad også at deltage i tvivlsomme nyhedsgrupper.

Vær varsom med at bruge Internetservices

På nettet findes uanede service-tilbud i form af nyhedsservices, mailinglister, diskussionsfora, chatsider og lignende.

Uden for arbejdstid er det tilladt at benytte disse internetservices, så længe du ikke skal hente og gemme filer fra internettet for at anvende disse services.

Hvis du deltager i internetservices, vil du typisk blive bedt om at indtaste personlige oplysninger, som for eksempel navn, adresse og e-postadresse. Oplysningerne registreres af internetudbyderen og bruges ofte til at distribuere

reklamemateriale mm. på trods af, at du aldrig har bedt om det. Det kaldes populært også for spam.

Birkerød Kommunes image

Når du er på job, må du ikke anvende internetservices, der kan skade Birkerød Kommunes image.

Husk på, at eventuelle indlæg i diskussionsfora og lignende udelukkende er et udtryk for din individuelle holdning og ikke nødvendigvis er i overensstemmelse med Birkerød Kommunes holdning.

Brug derfor din sunde fornuft, inden du udleverer personlige oplysninger til en hjemmeside. Du kan for eksempel stille dig selv spørgsmålene, om det er nødvendigt at lade sig registrere? Og om du har tillid til den pågældende internetudbyder?

Hvad registreres, når du er på internettet?

Normalt foretages der ikke kontrol af Birkerød Kommunes medarbejders anvendelse af internet.

Af sikkerhedsmæssige årsager, som for eksempel i forbindelse med en virustrussel, eller i særlige situationer, kan anvendelsen dog blive registreret.

Denne registrering vil kun blive foretaget af IT-organisationen og kun efter godkendelse fra kommunaldirektøren.



Regler & retningslinier for Brugerrettigheder



Sikkerhed
I BIRKERØD KOMMUNE

Brugerrettigheder skal sikre, at medarbejdere, som anvender Birkerød Kommunes IT-systemer har de nødvendige rettigheder til løsning af arbejdsopgaverne og at ingen har adgang til systemer og data, der arbejdsmæssigt ikke kan begrundes.

Generelle regler for rettigheder

Alle brugerrettigheder skal være skriftligt dokumenterede og henvendelser foretages via det elektroniske ansættelses/ændringsskema med afkrydsning af, om der er tale om oprettelse, ændring, sletning eller flytning. "Oprettelse" eller "Sletning" afkrydses, når der er tale om oprettelse eller sletning til systemer. Ændringer af rettigheder i systemer foretages ved hjælp af afkrydsning i "Ændring". Er der tale om intern rokering til anden arbejdsfunktion afkrydses "Flytning".

Alle brugerrettigheder skal godkendes af medarbejderens overordnede og systemejer. For de generelle systemer kan det være éngangsgodkendelser, hvor faste rettigheder tilknyttes faste arbejdsfunktioner. I de tilfælde er det ikke nødvendigt med systemejerens godkendelse. I forbindelse med god-

kendelse af brugerrettigheder, forholder systemejer sig til, om rettighederne kan begrundes i arbejdsmæssig sammenhæng. Der vurderes på relevansen af den ønskede rettighed med en skelnen mellem rettighed til at læse, rette, oprette og slette.

Desuden vurderer systemejer, om én rettighed medfører tildeling af andre rettigheder. Det kan for eksempel være i tilfælde af rettigheder til systempuljer. Systemadministrator udfører og kvitterer for oprettelsen af ansættelses/ændringsskemaet ved at udskrive og gemme dokumentationen i "IT MAPPE".

Administrator giver besked herom til den pågældende afdeling. Alle skemaer arkiveres, så længe en bruger er ansat i kommunen, og opbevares ét år efter fratæden. Arkivering sker i datoorden. Godkendelses- og oprettelsesprocedurene skal foretages af forskellige personer, så godkendende part ikke samtidig har mulighed for at tildele brugerrettigheder i systemet.

Oprettelse af brugerrettigheder

Når en bruger 1. gang tildeles rettigheder til ét eller flere systemer, er det

en oprettelse. I ansættelsesdatabasen anføres, hvilke systemer og hvilke profiler/rettigheder brugeren skal tildeles.

"Andet" angiver særlige systemer, som generelt ikke anvendes i kommunen. For disse systemer skal systemnavnet anføres. Brugeren tildeles ved oprettelsen en éngangsadgangskode, som skal ændres efter ibrugtagelsen.

Ændringer i eksisterende rettigheder

Ændringsproceduren anvendes, når en medarbejder skal have ændret eller ajourført rettighederne til ét eller flere systemer, som medarbejderen i forvejen har rettigheder til. Dette skal også ske ved anvendelse af ansættelses/ændringsbasen med en angivelse af, at der er tale om en ændring. Desuden afkrydses eller anføres det pågældende system, og der angives hvilke profiler eller adgange, der skal oprettes og/eller slettes.

Såfremt der er tale om en generel ændring i adgangen til et system, og som berører flere brugere, kan systemejer én gang for alle godkende ændringerne. Herefter iværksættes ændringerne for alle berørte brugere.