BALLERUP KOMMUNE

POLITIK OG ORGANISATION
Digitalisering og Forretningsudvikling

Dato: 16. november 2021

E-mail: amb2@balk.dk
Kontakt: Amanda Geisler Berglund

Sagsid: 85.10.00-P20-1-17

Anbefalinger til god databeskyttelse for kommunalpolitikere

10 anbefalinger om databeskyttelse for kommunalpolitikere

1. Opret et nyt og stærkt password

Beskyt dig selv ved at oprette et nyt password, som du kun bruger til dit kommunalpolitiske arbejde. Genanvend ikke passwords fra tidligere.

2. Udlevér aldrig dit password til andre

Dit password er personligt og må aldrig deles. Hvis andre får adgang til din konto kan de læse og sende beskeder i dit navn.

3. Brug ikke dit login flere steder

Brugen af sin kommunale profil på andre hjemmesider og platforme øger risikoen for hackerangreb og misbrug betragteligt og bør helt undgås.

4. Lås din tablet/smartphone

Når du forlader en digital enhed, bør du altid låse skærmen, så man kun kan tilgå oplysninger ved hjælp af dit personlige password.

5. Lån ikke din enhed ud – heller ikke til børn

Du er ansvarlig for de data, der opbevares på din enhed. Det kan fx være e-mails eller dokumenter, som kan indeholde persondata på borgere eller informationer, der er fortrolige.

6. Undgå personoplysninger, når du skriver e-mails

Har en borger skrevet en mail til dig med personoplysninger, så formulér dit svar uden personoplysninger, fx: ”Jeg har modtaget din mail og går videre med sagen”. Så minimerer du mængden af persondata, der opbevares på din enhed og – hvis uheldet er ude – kan havne i de forkerte hænder.

7. Slet e-mails med personoplysninger
Har du modtaget eller sendt mails med personoplysninger, bør du slette disse, hurtigst muligt – helst umiddelbart efter modtagelse eller afsendelse af mailen.

8. Undgå SMS kommunikation
Undgå at skrive SMS'er med personlige personoplysninger og skriv aldrig beskeder der indeholder følsomme personoplysninger. SMS-kommunikation er i høj risiko for datalæk.

9. Undgå altid chatfunktionerne på sociale medier
Chatfunktioner er dobbelt problematiske; Ligesom SMS er de en usikker kommunikationskanal, men derudover får de fleste sociale medier adgang til indholdet i beskeder, og dermed giver man tjenester som Facebook og Google adgang til data. Hvis en borger henvender sig på SMS, chat eller kommentarspor kan du foreslå e-mail eller et telefonopkald for at vejlede borgeren i sikker kommunikation og undgå, at fortrolige eller følsomme personoplysninger bliver delt på usikre kommunikationskanaler.

10. Download ikke apps på din kommunale enhed
Undgå installerede apps på sin kommunale enhed. Brug browseren eller en privat enhed. Hvis en app er installeret på en enhed, hvorpå der ligger oplysninger i din kommunale mail er der en risiko for, at fortrolige oplysninger havner hos tjenesteudbyderen. Ved kun at tilgå tjenesten via browseren sikrer du, at app'en ikke får adgang til alt indhold på dine enheder.

Anmeld hvis du har mistanke om et sikkerhedsbrud
Har du mistanke om at du er blevet hacket eller at nogen, der ikke burde, har fået adgang til data på din enhed? Henvend dig uden tøven til IT-Servicedesken på 2552 8008 for at få låst din konto. Hvis det er uden for åbningstiden kontakt da Digitaliseringschef Jens Kjellerup jeh2@balk.dk, 2477 4242.

Særligt for dig, der både er ansat og politiker i Ballerup Kommune
Når du både er ansat og politiker i kommunen, anvender du samme mailadresse. Bemærk, at der gælder andre regler for kommunens ansatte end for en kommunalpolitiker. Hvis du, ved siden af det politiske arbejde, også er ansat i kommunen, skal du være opmærksom på, at du er underlagt de samme regler som andre ansatte i kommunen, når du agerer som ansat i kommunen.

For at skelne mellem, hvornår du agerer som hhv. politiker og ansat, kan du adskille dette ved at gemme din politiske korrespondance i en mappe du giver navnet "Privat". Korrespondancen i mappen "Privat" vil af administrationen blive behandlet som fortrolig. Administrationen har ikke indsigt i denne korrespondance.