Kontakt
databeskyttelsesrådgiveren

Telefon 29 26 11 26
E-mail: dbr@faxekommune.dk

IT-sikkerhed

Sikkerhedsbrud

- og sikkerhedshændelser

Faxe Kommune gør et stort arbejde for, at du som medarbejder eller leder trygt kan benytte de systemer og det udstyr vi stiller til rådighed.

Men organisationen kan ikke blive 100 % sikker som moderne IT-rettet virksomhed med mindre du, som bruger, følger vores retningslinjer.

Du har pligt til at orientere dig om IT sikkerheden på din arbejdsplads.

Denne folder har vi fremstillet for at hjælpe dig med at overholde den nye lovgivning - og dermed undgå sikkerhedsbrud.

Overtrædelse af reglerne vil, i særlig grelle tilfælde, kunne tolkes som pligtforsømmelse og kan få ansættelses-mæssige konsekvenser.

Hvis noget går galt
- kontakt STRAKS IT Servicedesk

Mistanke om sikkerhedsbrud

Kontakt STRAKS IT Servicedesk
Hvis du får mistanke om et brud på persondata-sikkerheden eller informationssikkerhedspolitikken skal du STRAKS kontakte IT Servicedesk. Servicedesk kan hjælpe med at stoppe bruddet hurtigst muligt.

Kontakt databeskyttelsesrådgiveren (DBR)
Når du har kontaktet IT servicedesk skal
Du informere databeskyttelsesrådgiveren.
Ring på 56 20 37 07 / 30 84 30 74.
DBR vil stille dig en række spørgsmål for at vurdere bruddets omfang og risikoen forbundet med bruddet.
Det er DBRs opgave at vurdere næste skridt, herunder om bruddet skal anmeldes til Datatilsynet. Som udgangspunkt er næste skridt at involvere de relevante ledere.

Anmeldelse til Datatilsynet
Skal ske senest 72 timer efter bruddet er sket. Derfor er det vigtigt, at du STRAKS kontakter Servicedesk og ikke venter på at tale med din leder om det.

Informer din leder
Når du har talt med DBR skal du informere din nærmeste leder om sikkerhedsbruddet og din rolle i forhold til opgaven. DBR vurderer hvornår og i hvilket omfang ledelsen skal involveres.

IT Servicedesk
56 20 38 00
servicedesk@faxekommune.dk

Databeskyttelses rådgiveren
29 26 11 26
dbr@faxekommune.dk

Brud på persondatasikkerheden er f.eks.:

Kontakt Servicedesk og DBR i disse situationer
- Hacking, virusangreb, hul i firewall, brud på servere **AKUT**
- Personoplysninger bliver sendt til en forkert modtager **AKUT**
- Personoplysninger bliver sendt som usikker post **AKUT**
- Personoplysninger bliver offentliggjort (f.eks. på hjemmesiden) **AKUT**
- Uvedkommende personer får adgang til personoplysninger **AKUT**
- Personoplysninger bliver slettet ved et uheld **AKUT**
- Personoplysninger bliver tilintetgjort **AKUT**
- Hvis vi i en periode ikke har adgang til personoplysninger **AKUT**
  Det kan f.eks. være pga. hændeligt uheld som brand eller oversvømmelse
- Uvedkommende får adgang til personoplysninger pga. manglende kryptering af hjemmeside **AKUT**
- Vi indhenter oplysninger, vi ikke har lovhjemmel til/brug for til vores sagsbehandling – f.eks. fordi et system er opbygget, på en måde så man ikke kan komme videre uden at indtaste oplysningerne
- Flere forgæves forsøg på login
- Du har adgang til oplysninger i et system, som du ikke skal bruge for at kunne løse dine arbejdsopgaver
- Samme dokument er gemt flere steder – f.eks. fordi mail eller et dokument på et drev er ikke slettet efter journalisering
- Der er ikke adgang til personoplysninger, fordi de ikke er journaliseret
- Du har glemt at låse din pc-skærm eller telefon
- Du har delt din adgangskode med andre.

Konsekvenser ved brud på reglerne
Hvis du får kendskab til brud på kommunens sikkerhedspolitik, har du pligt til at melde det til IT Servicedesk.

Hvis du er i tvivl om noget er et brud på kommunens sikkerhedspolitik så skriv eller ring til IT Servicedesk.