# *Halsnæs Kommune*

## ***Informationssikkerhedspolitik***

Marts 2022

Halsnæs Kommune

*Oplev det rå og autentiske Halsnæs*

# Informationssikkerhedspolitik

**Indledning**
Det er et krav, at Halsnæs Kommune som dataansvarlig myndighed sikrer beskyttelse af personoplysninger. Byrådet har det endelige politiske ansvar for, at kommunen håndterer borgeres, virksomheders og øvrige offentlige myndigheders informationer på betryggende vis.

Dette dokument beskriver Halsnæs Kommunes overordnede informationssikkerhedspolitik. Denne politik sætter rammerne for operationel organisering og styring af informationssikkerhed, der udmøntes i etableringen af fastsatte regler og procedurer for kommunes informationssikkerhedshåndtering. Hermed etableres grundlaget for det daglige arbejde med informationssikkerhed inden for kommunens virke.

Politikken omfatter informationer i såvel digital som fysisk format samt informationsaktiver.

**Mål for sikkerhedsniveau**
Halsnæs Kommune fastlægger på baggrund af konkrete risikovurderinger et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer og systemer. Sikkerhedsniveauet og anvendelsen skal dels være i overensstemmelse med gældende lovgivning, dels være fleksibel og justeres ud fra aktuelle risiko- og omkostningsvurderinger.
Ved fastlæggelse af sikkerhedsniveauet tages der udgangspunkt i 3 begreber:

*Fortrolighed*
Borgerne skal til enhver tid kunne stole på, at de trygt kan overlade deres følsomme og fortrolige personoplysninger til Halsnæs Kommune. Informationssikkerhed skal sikre fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

*Integritet*
Informationssikkerhed skal sikre pålidelig og korrekt brug af løsningerne og minimere risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefra kommende hændelser.

*Tilgængelighed*
Informationssikkerhed skal være medvirkende til, at vi opnår høj tilgængelighed og minimere risiko for nedbrud på vores systemer.
Halsnæs Kommune skal dermed træffe nødvendige foranstaltninger til at beskytte oplysninger mod uautoriseret anvendelse, fejl i de registrerede eller behandlede oplysninger, og til at sikre den højst mulige ”oppetid” for vores løsninger.

**Holdninger og principper**
Halsnæs Kommune vil fastlægge informationssikkerheden, så der dels tages hensyn til ønsket om høj sikkerhed, dels hensynet til brugervenlig it-anvendelse og omkostningerne ved investering i sikkerhed.

Sikkerhedsforanstaltninger kan til tider opleves som en barriere for medarbejdernes daglige anvendelse af IT. Her vil Halsnæs Kommune sikre medarbejdernes forståelse for nødvendigheden af disse foranstaltninger, så at sikkerhed bliver en naturlig del af arbejdet i kommunen.

Kommunen vil løbende arbejde med at informere og uddanne medarbejderne, så de får de nødvendige

kompetencer, til at sikre at informationssikkerheden kan overholdes samtidig med at arbejdet kan udføres så effektivt som muligt.

**Gyldighed og omfang**
Informationssikkerhedspolitikken er gældende for

- Alle ansatte i Halsnæs kommune
- Medlemmer af byrådet – under hensyntagen til de særlige rettigheder og forpligtelser, som i øvrigt gælder for byrådsmedlemmer
- Andre folkevalgte der har adgang til kommunale data
- Samarbejdspartnere og leverandører af informationssikkerhedsydelser
- Eventuelle andre brugere af Halsnæs kommunes datanetværk

Kommunens informationssikkerhed gælder for alle lokaliteter, hvor der sker en anvendelse og bearbejdning af kommunens informationer, dvs. rådhus, kommunale virksomheder, fjernarbejdspladser, adgang via mobile enheder mv.

For leverandører, som har adgang til kommunens systemer gælder det, at de skal have implementeret et sikkerhedsniveau, der mindst svarer til kommunens niveau. Dette sikres ved indgåelse af databehandleraftaler.

**Ansvarsplacering**
Chefgruppen har det overordnede ansvar for informationssikkerheden, herunder udpegning af rollerne i sikkerhedsarbejdet.
Kommunens ledere har ansvaret for sikkerheden og uddelegerer opgaver og ansvar vedrørende de enkelte funktionsområder, herunder også for vejledning og instruktion af medarbejdere.
Enhver medarbejder og folkevalgt ved kommunen har således et medansvar for informationssikkerheden.

**Adgangsstyring**
Alle informationsaktiver skal i nærmere specificeret omfang være beskyttet imod uautoriseret adgang.
Der skal kunne udføres adgangskontrol og - via logning - skabes grundlag for efterkontrol.

**Funktionsadskillelse**
Der etableres i fornødent omfang regler for funktionsadskillelse (dvs. den samme person må ikke både udføre og godkende en given handling eller funktion). Dette princip er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser fra fejl, uheld og bevidst negative handlinger forårsaget af enkeltpersoner.

**Uafhængighed af enkeltpersoner**
Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig betydning for kommunen.

**Driftsforstyrrelser**
Skal imødegås gennem:

- Forebyggende foranstaltninger, bl.a. procedurer for kvalitetssikring, ændringsstyring og dokumentations-vedligeholdelse.
- Problemhåndtering, bl.a. procedurer for skadeudbedring, omgåelse mm. på en sådan måde, at de aftalte tilgængelighedskrav ikke overskrides.

**Katastrofesituationer**
Omfanget af foranstaltninger besluttes på basis af foretaget risikovurdering. Hvor risikoanalysen berettiger dette, skal der udarbejdes beredskabsplaner.
Katastrofer forårsaget af brand- eller vandskader søges primært undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr.
Der skal foreligge beredskabsplaner for de nødsituationer, der af Chefgruppen er defineret som kritiske.

**Udmøntning af informationssikkerhedspolitikken**
Informationssikkerhedsregler og -procedurer udarbejdes i overensstemmelse med politikken, EU's databeskyttelsesforordning samt principperne i den internationale ISO standard for informationssikkerhed. Regler og procedurer skal gennemgås hvert år som fastlagt i årshjul for informationssikkerhedsarbejdet.

**Afvigelser fra informationssikkerhedspolitikken**
Chefgruppen kan efter indstilling fra den øverste daglige Informationssikkerhedsleder - i enkeltstående tilfælde foretage afvigelser fra denne informationssikkerhedspolitik.

**Overtrædelse**
Bevidst eller ubevidst overtrædelse af kommunens informationssikkerhed kan blandt andet medføre, at borgernes oplysninger kompromitteres.
Overtrædelse af informationssikkerheden skal rapporteres, og er den daglige leders ansvar.

**Gyldighed**

Denne overordnede politik skal godkendes af Byrådet og revurderes efter behov, dog mindst hvert 4. år.
En gang årligt skal Byrådet have forelagt status på informationssikkerheden – årsrapport fra kommunens databeskyttelsesrådgiver samt it-revisionsrapport. Ved større sikkerhedshændelser informeres Byrådet straks.

Byrådet godkender endvidere valg af leverandører til meget store fælleskommunale it-anskaffelser.

Godkendt af Halsnæs Kommunes byråd

**Halsnæs Kommune**
Rådhuspladsen 1
3300 Frederiksværk
Telefon 51 49 59 85