Aabenraa Kommune

Informationssikkerhedspolitik

1. Indledning

Informationssikkerhedspolitikken udstikker en fælles og ansvarlig retning for, hvordan Aabenraa Kommune beskytter data og IT-systemer mod uautoriseret adgang, fejl og misbrug. Politikken er forankret i kommunens øverste administrative ledelse og danner grundlag for en robust og ansvarlig digital forvaltning sikrer, at arbejdet med informationssikkerhed skaber rammerne for sikker anvendelse af IT.

Sikker anvendelse skal understøtte borgerens og samfundets tillid til kommunens digitale tjenester.

Politikken gælder for alle med adgang til kommunens data og IT-systemer.

2. Målsætninger for informationssikkerhed

Aabenraa Kommune tilpasser løbende indsatsen for informationssikkerhed efter den teknologiske udvikling, de ressourcer, der er til rådighed, og den måde kommunen arbejder med data på. Målet er at sikre et passende og tidssvarende niveau af beskyttelse for data og IT-systemer. Derfor forpligter kommunen sig til at:

- Beskytte fortrolighed, integritet og tilgængelighed af data og IT-systemer mod hændelser og angreb
- Minimere sandsynlighed for sikkerhedshændelser, der fører til driftsforstyrrelser og databrud
- Minimere konsekvensen af sikkerhedshændelser til et acceptabelt niveau.

3. Organisering og ansvar

Kommunens øverste administrative ledelse har ansvaret for informationssikkerhed.

Direktionen har ansvaret for informationssikkerheden i Aabenraa Kommune. Direktionen har uddelegeret dette til Informationssikkerhedsudvalget (ISU), der på vegne af Direktionen sætter mål, regelmæssigt orienteres om status og tager stilling til kommunens informationssikkerhed.
ISU har derfor det koordinerende ansvar for kommunens sikkerhedsniveau, og udmønter dette via politikker, processer, procedurer, retningslinjer og foranstaltninger. Stabsdirektøren er formand for ISU.
IT-Afdelingen har det operationelle ansvar for kommunens tekniske informationssikkerhed og omsætter retningslinjer og politikker til konkrete foranstaltninger. IT-Afdelingen sikrer, at den digitale infrastruktur drives sådan, at både hensyn til en stabil daglig drift og sikkerhedshensyn bliver varetaget.

Ansvar for at beskytte data og IT-systemer er et fællesanliggende, der kræver engagement og opmærksomhed for alle medarbejdere og ledelseslag. Roller og ansvar beskrives nærmere i kommissorier.

4. Risikotolerance og sikkerhedsniveau

Risikotolerance er det risikoniveau, som kommunen er villig til at tolerere. Sikkerhedsniveau er kommunens minimumskrav til sikkerhedsforanstaltninger.

Aabenraa Kommunes sikkerhedsniveau baseres på risikotolerancen, og fastlægges derfor ud fra en vurdering af de risici, som kommunen ønsker at reducere til et acceptabelt niveau. Vurderingen revideres løbende for at kommunen tidssvarende kan forholde sig til et dynamisk trusselslandskab. Grundlaget for vurderingen er kommunens risikotolerance, lovgivning og anerkendte standarder (fx ISO 27001). Overordnede risikovurderinger gennemføres løbende og ved ændringer i trusselsbillede, teknologi eller forretningsgange. Vurderingerne dokumenteres og danner grundlag for at ISU udvælger nye og justerer nuværende kontroller.

Informationssikkerhedsudvalget har ansvar for at følge op på resultater og sikre, at passende foranstaltninger besluttes og implementeres.

For at kunne omsætte kommunens risikotolerance og sikkerhedsniveau til konkrete og tilpassede krav, er det nødvendigt at styre risici, og klassificere IT-systemer og data.

a. Risikostyring:

Der er implementeret risikostyring som sikrer passende tekniske og organisatoriske foranstaltninger til håndtering af risici, som truer sikkerheden i net- og informationssystemer. Disse foranstaltninger sker på baggrund af en risikovurdering, og sikrer dermed proportionalitet i forhold til de identificerede trusler og sårbarheder.

En risikovurdering indeholder en vurdering af, om en aktivitet har konsekvenser for:

- Den registrerede
- Aabenraa Kommune og
- Samfundet.

b. Klassifikation

Informationer, data og IT-systemer klassificeres efter krav til fortrolighed, integritet og tilgængelighed. Dette afgør, hvilke beskyttelsesforanstaltninger der er nødvendige ift. tilsyn, adgang, opbevaring og sletning.

Klassifikationen omfatter:

- **Personoplysninger**: Følsomme (art. 9), fortrolige (art. 10, særlovgivning) og almindelige (art. 6)
- **Kritikalitet af IT-systemer:** Samfundskritisk, essentielt, væsentligt og uvæsentligt. Kritikaliteten afgøres ved en vurdering af om en hændelse, nedetid og lignende i systemet, vil forhindre kommunen i at varetage en samfundskritisk funktion.

5. Adfærd og awareness

Sikker digital adfærd er en forudsætning for sikker drift og beskyttelse af borgernes data. Alle medarbejdere bliver instrueret i retningslinjer og regler, der efterlever kommunens politik for informationssikkerhed.

Alle medarbejdere bliver tilbudt træning i sikker digital adfærd. Særlige målgrupper, herunder ledelse og IT-Afdelingen modtager målrettet uddannelse i forhold til funktion.

6. Fysisk sikkerhed og it-udstyr

Kommunen beskytter fysiske områder og IT-udstyr for at forhindre uautoriseret adgang, beskadigelse, misbrug og tyveri.

Beskyttelse af bygninger, områder og fysisk adgang fastsættes under hensyn til den aktuelle risiko og ønsket om åbenhed og tilgængelighed for borgerne.

Kritisk IT-udstyr skal i vidst muligt omfang placeres i særligt sikrede områder, med adgangsbegrænsning.

7. Styring af netværk og drift

Kommunens netværk og IT-drift understøtter en stabil, sikker og tilgængelig digital infrastruktur, som beskytter mod tab, misbrug og uautoriseret adgang.
Netværk er en vital del af kommunens digitale infrastruktur, der derfor skal beskyttes for at sikre stabil drift og for at værne om kommunens IT-systemer og data.

Som en forudsætning for at kommunens digitale infrastruktur er modstandsdygtig overfor udfald, hændelser og angreb fra ondsindede aktører, er der etableret foranstaltninger og procedurer. Disse foranstaltninger og procedurer forebygger driftsforstyrrelser, og vedligeholdes.

For at beskytte kommunens IT-systemer og data i den daglige drift anvendes tre centrale sikkerhedselementer: logning, adgangsstyring og kryptering.

a. Logning og logkontrols

Kommunen fører log over brugen af IT-systemer og netværk for at opdage misbrug, efterforske hændelser og understøtte revisionsspor. Logning sikrer sporbarhed og understøtter både datasikkerhed og ansvarlighed.

- Krav til logning afgøres blandt andet på baggrund af systemets klassifikation.
- Procedure for kontrol af logfiler afgøres på baggrund af en konkret risikovurdering
- Adgangen til logdata er begrænset og styret af rolleadskillelse og fortrolighed.

b. Adgang og rettigheder til data og IT-systemer

Følsomme og kritiske IT-systemer og data beskyttes mod uautoriseret adgang og ændring, uanset hvor de befinder sig. Derfor beskyttes alle IT-systemer med adgangskontrol. Der anvendes i videst muligt omfang multifaktor-login til systemer med følsomme eller fortrolige data.

- Adgang til data minimeres og afspejler et arbejdsbetinget behov.
- Der er funktionsadskillelse imellem bestiller, bruger og administrator af adgange og rettigheder til IT-systemer og data.
- I fagsystemer, der kræver en godkendelse, er der funktionsadskillelse mellem roller som rekvirent, bestiller og roller som godkender og administrator.
- Det er et krav, at adgang til og ændringer af følsomme eller kritiske IT-systemer og data kan spores til en unik identitet.

c. Kryptering

Kryptering anvendes for at beskytte fortrolighed af filer og data, og sikrer imod uautoriseret adgang til kommunens filer og data. Hvor det er relevant, beskytter kryptering integritet af data.

- Kryptering bliver altid anvendt ved overførsel af filer og data.
- Kryptering bliver anvendt ved lagring af følsomme og kritiske data.
- Der anvendes hverken forældede eller svage algoritmer og protokoller til kryptering.
- Krypteringsnøgler opbevares forsvarligt.

8. Anskaffelse, udvikling og vedligeholdelse af IT-systemer

Der er sikkerhedskrav til leverandører og samarbejdspartnere, der leverer kritiske IT-systemer. Sikkerhedskravene afhænger af IT-systemets klassifikation.

Sikkerhedskrav og klassifikation bliver fastlagt i en risikobaseret vurdering, når et IT-system anskaffes eller videreudvikles.
IT-visitationen har faste processer for anskaffelse og videreudvikling og faciliterer vurderingen.

Alle IT-systemer har en systemejer. Systemejer har ansvar for, at IT-systemet lever op til sikkerhedskrav. Ved væsentlige ændringer kan systemejer inddrage IT-visitationen igen.

9. Håndtering af sikkerhedshændelser

Der er processer og procedurer for håndtering af IT-sikkerhedshændelser og brud på persondata.
En hændelse klassificeres som IT-sikkerhedshændelse, når der er begrundet mistanke om bevidst brud på fortrolighed, integritet eller tilgængelighed.

Brud på persondata omfatter derudover den utilsigtede tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Alle medarbejdere har pligt til at indberette en IT-sikkerhedshændelse og brud på persondata, når de får kendskab til hændelsen.
Ved IT-sikkerhedshændelser eller databrud, der udgør en risiko for den registrerede eller et væsentligt nedbrud i samfundskritiske IT-systemer, vil relevante tilsynsmyndigheder blive underrettet.

10. Beredskab

Aabenraa Kommunes beredskab udgør en væsentlig del af kommunens evne til at være modstandsdygtig overfor nedbrud og væsentlige hændelser.

Aabenraa Kommunes samfundskritiske systemer har planer for reetablering, driftskontinuitet og krisehåndtering. Planerne anvendes i forbindelse med væsentlige hændelser.

Kommunen har udarbejdet en IT-beredskabsplan for, hvordan man begrænser konsekvenser af datatab og nedbrud i IT-systemer som følge af evt. katastrofer og væsentlige hændelser.

IT-beredskabsplanen testes periodisk og vedligeholdes, for at sikre tidssvarende og effektiv IT-beredskab.

Efter hver test eller hændelse hvor beredskabsplanen har været aktiveret, bliver responsen evalueret, og forbedringspunkter dokumenteres og implementeres.

IT-beredskabet indgår i Aabenraa Kommunes overordnede kriseberedskab.

11. Revision

Mindst én gang om året gennemføres gennemgang af politikker, processer, procedurer og foranstaltninger, hvor overensstemmelse med GDPR, NIS2 og øvrig relevant lovgivning vurderes.

Behandlingen kan en revidering kan føre til behov for at ændre politikken.

- Mindre og redaktionelle bliver ændringer håndteret administrativt og orienteres i ISU
- Væsentlige ændringer behandles i ISU med henblik på godkendelse i Direktion.

12. Godkendelse

Informationssikkerhedspolitikken godkendes af Direktionen.

13. Ændringslog

Årsag til revision Beskriv kort, hvad der er tilpasset og hvorfor	Dato
Første version er godkendt	15-12-2025

Version:	Ansvarlig for vedligeholdelse	Revisionshyppighed
1.0	IT-afdelingen, ISU	Årligt og ved væsentlige ændringer i forretningsmæssige mål og trusselsbillede.
Ref til ISO 27002	Godkendt af:	Godkendt den:
5.01	Direktionen	

Målgruppe: Alle