IT- og Informationssikkerhed: Håndbog for Ledere og Systemejer

1. Forord

En Systemejer er den, der har ansvar for systemer, og derfor også er ansvarlige for de data, systemet behandler. I Aabenraa Kommune er det ledere på chef niveau, der er systemejere, fx er IT-chefen systemansvarlig for de systemer, IT-afdelingen udbyder til Aabenraa Kommunes organisation.

Systemejer ansvaret medfører en række ansvarsområder, der skal varetages. De ansvarsområder kan uddelegeres, fx til en systemansvarlig medarbejder eller superbruger, men det er systemejeren, der har ansvaret.

2. Introduktion

Som leder og systemejer i kommunen har du et særligt ansvar for at sikre, at IT-systemer og data håndteres sikkert og i overensstemmelse med kommunens informationssikkerhedspolitik.

Denne håndbog giver et overblik over dine forpligtelser og de retningslinjer, du skal følge for at efterleve informationssikkerhedskravene.

3. Ledelsens ansvar for informationssikkerhed

3.1 Implementering af sikkerhedspolitik

- Du er ansvarlig for at sikre, at medarbejdere i dit ansvarsområde kender til og overholder kommunens informationssikkerhedspolitik. Dette inkluderer at motivere medarbejdere til at følge retningslinjerne og skabe bevidsthed om deres roller i forhold til sikkerheden.
- Det er dit ansvar, at der sker løbende opfølgning på, hvordan sikkerhedspolitikken overholdes inden for de systemer, du er ansvarlig for, især når det gælder risikovurdering og autorisationskontrol.

3.2 Godkendelse og opfølgning

- Sikkerhedspolitikken godkendes af Økonomiudvalget hvert andet år, men som leder og systemejer skal du sikre, at politikken bliver fulgt i dagligdagen.
- Mindst én gang om året skal du følge op på, hvordan kritiske systemer efterlever sikkerhedspolitikken. Dette inkluderer kontrol af autorisationer og opdatering af systemernes risikovurderinger.

4. Systemejerens ansvar for adgang og data

4.1 Adgangskontrol

- Som systemejer har du ansvar for at definere, godkende og løbende revurdere adgangsrettigheder for de medarbejdere, der bruger systemet. Det sikrer, at kun relevante medarbejdere har adgang til følsomme eller kritiske data.

- Du skal sørge for, at adgangsrettighederne stemmer overens med de arbejdsopgaver, den enkelte medarbejder har, og at rettighederne fjernes, når en medarbejder ikke længere har behov for dem (f.eks. ved fratrædelse eller omplacering).

4.2 Kryptering og databeskyttelse

- Sørg for, at alle fortrolige data i dit system er korrekt krypteret, både under opbevaring og transmission. Det er din opgave at sikre, at følsomme oplysninger kun er tilgængelige for autoriserede personer.
- Alle udvekslinger af data med eksterne parter skal være beskyttet af en fortrolighedsaftale eller databehandleraftale, som opbevares i kommunens systemer.

5. Systemadministratorer og systemejere

5.1 Ledelsestilsyn

- Systemejer skal årligt gennemgå listen over medarbejdere med systemadministrator adgang til kritiske systemer.

5.2 Funktionsadskillelse

- Risiko for misbrug af systemadgange skal minimeres ved at benytte funktionsadskillelse, så det ikke er samme medarbejder, der har systemadministrator adgange, også skal kontrollere egne behov adgange og overvåge handlinger.
- Systemadministrator og systemejer for kritiske systemer skal derfor ikke være samme medarbejder.

6. Risikovurdering og sårbarhedsstyring

6.1 Løbende risikovurderinger

- For at sikre systemernes robusthed er det din opgave som systemejer at gennemføre regelmæssige risikovurderinger. Disse vurderinger skal identificere potentielle sårbarheder, trusler og risici forbundet med systemets drift.
- Alle systemer, der behandler personoplysninger, skal have en opdateret risikovurdering, som dokumenteres og opbevares i kommunens ESDH-system.

6.2 Trusselsopdateringer

- Du skal holde dig orienteret om nye trusler og sårbarheder, som kan påvirke systemet. IT-afdelingen vil informere dig om relevante sikkerhedstrusler, men det er dit ansvar at handle hurtigt for at minimere risici for systemet.

7. Outsourcing og tredjepartsadgang

7.1 Outsourcing af systemer

- Ved outsourcing af IT-systemer er det vigtigt at sikre, at sikkerhedsniveauet hos outsourcing-partneren lever op til kommunens krav. Dette skal godkendes før

indgåelse af kontrakten, og partnerens sikkerhedsniveau skal vurderes regelmæssigt.
- Sørg for, at der foretages ekstern revision af outsourcing-partneren mindst én gang om året, og at resultatet dokumenteres i kommunens ESDH-system.

7.2 Tredjepartsadgang

- Du skal sikre, at enhver tredjepart, som får adgang til kommunens data, har underskrevet en fortrolighedsaftale eller databehandleraftale.
- Disse aftaler skal opbevares korrekt og revideres regelmæssigt for at sikre, at sikkerheden overholdes.

8. Overvågning og hændelseshåndtering

8.1 Systemovervågning

- Som systemejer skal du sikre, at der er implementeret tilstrækkelig overvågning af systemets aktiviteter, herunder logning af brugeradgang og systemændringer. Logfiler skal opbevares i mindst tre måneder og være tilgængelige ved behov for efterforskning eller audit.
- Alle driftskritiske systemer skal løbende overvåges for at sikre, at systemets tilgængelighed og kapacitet ikke kompromitteres.

8.2 Håndtering af sikkerhedshændelser

- Du er ansvarlig for, at sikkerhedshændelser i systemet bliver rapporteret straks til IT-afdelingen og databeskyttelsesrådgiveren. Dette gælder uanset om det er et brud på fortrolighed, integritet eller tilgængelighed.
- Opfølgning på sikkerhedshændelser skal ske systematisk, og du skal evaluere, om der er behov for justeringer i systemets sikkerhed eller procedurer baseret på de hændelser, der er indtruffet.

9. Beredskabsplaner og fortsat drift

9.1 Planlægning af beredskab

- Beredskabsplaner skal være på plads for alle systemer, der er kritiske for kommunens drift. Planerne skal omfatte scenarier for både tekniske og organisatoriske nødsituationer, og de skal testes og opdateres mindst én gang om året.
- Som systemejer skal du sikre, at alle relevante medarbejdere er informeret om deres rolle i beredskabet, og at de er trænet i at reagere korrekt, hvis en beredskabsplan aktiveres.

9.2 Sikring af fortsat drift

- Nødplaner skal indeholde en beskrivelse af, hvordan forretningskritiske systemer kan genetableres hurtigt efter en større hændelse. Sørg for, at der er taget højde for opbevaring af sikkerhedskopier, eksterne samarbejdsaftaler og alternative driftslokationer.