Informasjonssikkerhet

Øyvind Rekdal, 17. mars 2015

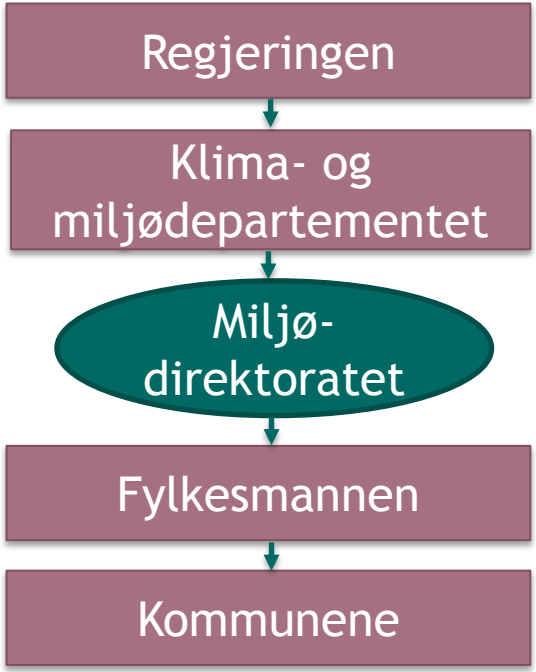
Om meg

- Øyvind Rekdal
- Utdannet sivilingeniør
- Jobber som seniorrådgiver i seksjon for virksomhetsutvikling i Miljødirektoratet
- Prosjektleder for å implementere styringssystem for informasjonssikkerhet
- Tidligere arkivleder i Direktoratet for naturforvaltning og i Miljødirektoratet

MILJØ-
DIREKTORATET

Dette er Miljødirektoratet

- forvaltningsorgan under Klima- og miljødepartementet
- etablert 1. juli 2013
- om lag 700 medarbeidere – hovedsakelig i Trondheim og Oslo



MILJØ-DIREKTORATET

Resultatområdene vi jobber med

- naturmangfold
- kulturminner og kulturmiljø
- friluftsliv
- forurensning
- klima
- polarområdene

Foto: Marie Lier

MILJØ-DIREKTORATET

Visjon

Rent og rikt miljø

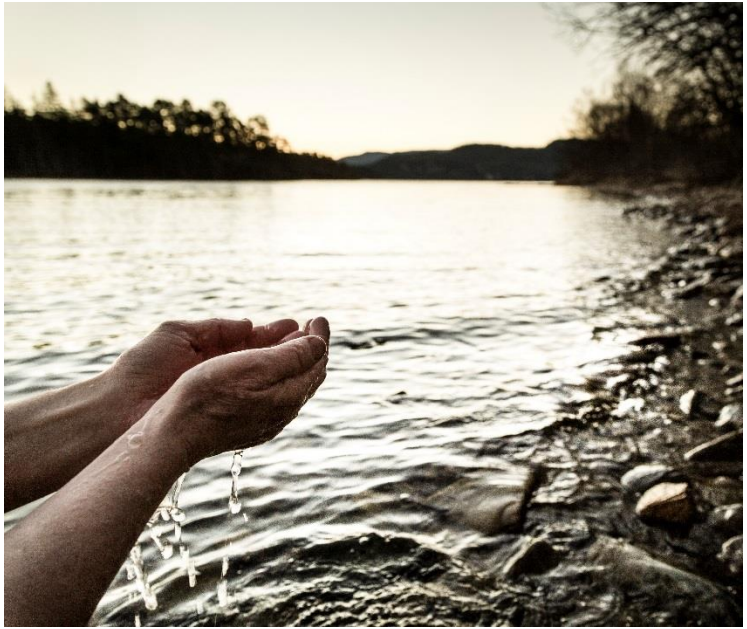


Foto: Thor Nielsen

MILJØ-
DIREKTORATET

Hva er informasjonssikkerhet?

"Tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet), og at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet)."

Datatilsynets definisjon

MILJØ-DIREKTORATET

Hva sier § 15 i e-forvaltningsforskriften?

«Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.»

MILJØ-DIREKTORATET

Hva er internkontroll?

Internkontroll slik DFØ har definert det:

«Internkontroll er en prosess, gjennomført av foretakets styre, ledelse og ansatte som er utformet for å gi rimelig sikkerhet vedrørende måloppnåelse innen følgende områder;

- Målrettet og effektiv drift
- Pålitelig rapportering
- Overholdelse av lover og regler»

MILJØ-DIREKTORATET

Hvem anbefaler standard og hva har blitt anbefalt

- Difi er gitt myndighet til å gi anbefalinger på informasjonssikkerhetsområdet
- Difi anbefaler i referansekatalogen å basere styringssystem for informasjonssikkerhet på ISO 27001(kun anbefaling, ikke krav)
- Det er mulig å sertifisere virksomheten på ISO 27001
- Difi utvikler for tiden en veileder for implementering av styringssystem basert på ISO 27001

MILJØ-DIREKTORATET

Hvorfor bør arkivet engasjere seg i informasjonssikkerhet?

- Forvalter enorme mengder av virksomhetens viktigste informasjon
- Mye av informasjonen i arkivene vil kreve ekstra fokus med hensyn på informasjonssikkerhet
- Unngå dobbeltarbeid ved å hente og gi gevinster fra det som gjøres i informasjonssikkerhetsarbeidet

MILJØ-DIREKTORATET

Sikkerhetsorganisering

- Har virksomheten en egen sikkerhetsorganisasjon? Er arkivet representert her?
- ISO 27001 krever at ansvar og myndighet for roller opp mot informasjonssikkerhet skal være tydelig kommunisert
- Kjenner dere i arkivet hvilke ansvar og myndighet dere har opp mot informasjonssikkerheten til virksomheten?

MILJØ-
DIREKTORATET

Informasjonssikkerhetspolicy

- Har virksomheten en egen informasjonssikkerhetspolicy? Gjør dere i så fall kjent med denne
- Baser rutiner og arbeid på det som står i informasjonssikkerhetspolicyen
- Informasjonssikkerhetsarbeidet må ses i sammenheng med virksomhetens kontekst

MILJØ-DIREKTORATET

Risikostyring

- Fra § 15 i e-forvaltningsforskriften - «Omfang og innretning på internkontrollen skal være tilpasset risiko»
- ISO 27001 er basert på risikostyring
- Er en egen ISO-standard for risikostyring; ISO 31000
- ISO 27005 er risikostyring rettet mot informasjonssikkerhet
- Bør gjøre verdivurdering og risikoanalyse av viktige system og prosesser. Dette gjelder for arkivsystem og dokumentflyt.

MILJØ-DIREKTORATET

Risikostyring

MILJØ-
DIREKTORATET

Informasjonsverdier

- ISO 27001 setter krav om å kjenne virksomhetens informasjonsverdier
- Arkivplanen er nyttig for de som skal få oversikt over informasjonsverdier
- Arkivet vil kunne få nytte av oversikt over informasjonsverdier i sitt bevarings- og kassasjonsarbeid

MILJØ-
DIREKTORATET

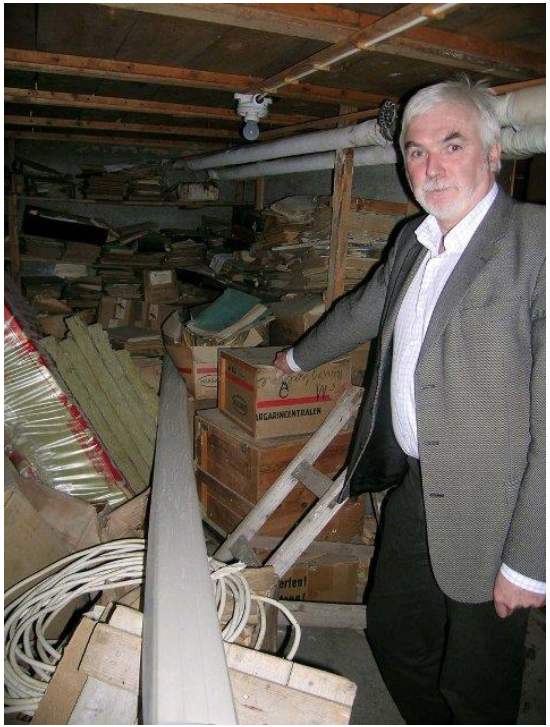
Oversikt over relevant lovverk

- Ta med arkivlov med forskrift i informasjonssikkerhetsarbeidet
- Flere lovverk er også relevante for arkivet

MILJØ-DIREKTORATET

Fysiske arkiv

Rådmannen viser frem Herøy kommune sine arkiv i 2007



Fysiske arkiv

- Husk fysiske arkiv i informasjonssikkerhetssammenheng
- Kravene til arkivlokaler er informasjonssikkerhetskrav
- For de som fortsatt har arkivlokaler som ikke følger kravene kan ISO 27001/informasjonssikkerhet være en mulig vinkling opp mot ledelsen

MILJØ-
DIREKTORATET

Avvik

- ISO 27001 og flere regelverk setter krav til systematisk avvikshåndtering
- Avvikshåndtering er et av de enkleste og minst resurskrevende virkemidlene til læring og forbedring
- Skap god kultur for å melde avvik

MILJØ-
DIREKTORATET

Lovverk med strenge krav til informasjonssikkerhet

- Sikkerhetslova
- Beskyttelsesinstruksen

MILJØ-DIREKTORATET

Oppsummering

- Arkivet må involvere seg i informasjonssikkerhet
- Informasjonssikkerhet er alles ansvar; ekstra bevissthet om dette i arkivet
- Tett samarbeid med IT og gjerne en IT-arkivar
- Bruk det dere har, ikke finn opp hjulet på nytt

MILJØ-
DIREKTORATET

MILJØ-
DIREKTORATET

www.miljødirektoratet.no