Innhold

[1. Omfang 1](#_Toc465148240)

[2. Formålet med vår informasjonsbehandling og informasjonssikkerhet 1](#_Toc465148241)

[3. Mål for informasjonssikkerhet 1](#_Toc465148242)

[4. Strategi for informasjonssikkerhet 1](#_Toc465148243)

[4.1 Organisering 1](#_Toc465148244)

[4.2 Krav til internkontroll- og sikkerhetsarbeidet 2](#_Toc465148245)

[4.3 Krav til ansatte 2](#_Toc465148246)

# Omfang

Denne policyen for informasjonssikkerhet gjelder all informasjonsbehandling som skjer internt i direktoratet og som direktoratet har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-verktøy er også inkludert.

# Formålet med vår informasjonsbehandling og informasjonssikkerhet

Formålet med informasjonsbehandling i direktoratet er å understøtte våre oppgaver og tjenester slik at vi kan nå våre mål og realisere vår visjon. Direktoratets mål og prioriteringer framkommer i vår overordnede strategi og virksomhets­plan. De er sammenfattet i vår visjon om «trivsel, vekst og trygghet».

En informasjons­behandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at direktoratet skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

# Mål for informasjonssikkerhet

Overordnet:

* Vår behandling av informasjon er i samsvar med lover, regler og avtaler, og bidrar på en formåls- og kostnadseffektiv måte til best mulig realisering av virksomhetens samlede mål

Tilgjengelighet:

* Relevant informasjon og hensiktsmessige IKT-løsninger er tilgjengelig på en effektiv måte for ansatte, innbyggere og næringslivet

Integritet:

* Informasjon som virksomheten har ansvaret for blir bare produsert og endret av ansatte eller eksterne som har fullmakt til dette
* Informasjon blir ikke endret utilsiktet

Konfidensialitet:

* Bare personer med innsynsrett og ansatte med tjenstlig behov får kjennskap til taushetspliktig informasjon
* Bare personer med innsynsrett og de ansatte som ledelsen har bestemt, får kjennskap til informasjon som virksomheten har unntatt offentlighet av andre grunner enn taushetsplikt

# Strategi for informasjonssikkerhet

## Organisering

* Ansvar og myndighet for informasjonssikkerhet skal følge det ordinære linjeansvaret
* Ledere som har ansvar for mål, arbeidsoppgaver og tjenester skal også ha ansvaret for tilhørende informasjonsbehandling, IKT-system og informasjonssikkerhet
* Nødvendige fellesfunksjoner, støttefunksjoner og samarbeidsgrupper skal etableres, ha tydelige roller og ansvar og understøtte linjelederne rundt om i virksomheten
* Systemeiere for fellessystem skal ivareta interessene til de som benytter systemene i sin oppgave­løsning, og involvere disse på hensiktsmessig måte i systemforvaltning og informasjonssikkerhets­arbeid
* Sikkerhetsarbeid skal være en integrert del av internkontrollarbeidet
* Internkontroll og sikkerhetsarbeid skal så langt det er hensiktsmessig være integrert på tvers av internkontrollområder

## Krav til internkontroll- og sikkerhetsarbeidet

* Arbeidet med informasjonssikkerhet skal være forankret i en internkontroll (styring og kontroll) basert på anerkjente standarder på informasjonssikkerhetsområdet
* Arbeidet skal følge gjeldende lover, regler og avtaler
* Vi skal systematisk vurdere behov for - og gjennomføre nødvendige risikovurderinger
* Risikoreduserende tiltak skal være basert på risikovurderinger, vesentlighet, nytte-kost vurderinger og ledelsens føringer for risikohåndtering og et effektivt sikkerhetsarbeid
* Hendelser som kan påvirke målene for informasjonssikkerhet negativt, skal meldes og følges opp på en systematisk måte
* Ledere på alle nivå skal systematisk styre, kontrollere og følge opp tilstanden og arbeidet med informasjonssikkerhet i egen enhet
* Arbeidet med informasjonssikkerhet skal evalueres systematisk

## Krav til ansatte

* Alle ansatte skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon de behandler og hvilke krav som stilles til informasjonsbehandlingen og bruken av IKT
* Alle ansatte skal etterleve de lover, regler, retningslinjer, krav, prosedyrer, rutiner mv. som gjelder for dem og det arbeid de utfører