***(Teksten merket gult her innledningsvis er en kommentar***

*Dette eksempelet er en enkel skisse til et notat som bør utarbeides innledningsvis i arbeidet med føringer for styring av informasjonssikkerhet. Innretning og omfanget på notatet må tilpasses virksomhetens egenart og de behov man mener å ha i det videre arbeidet med føringene.*

*Man bør spesielt vurdere om man skal gå nærmere inn på pkt. 6 «Andre internkontrollområder», se konkret på hva man har fra før der, for å ta stilling til om deler av føringene kanskje bør være felles for flere eller alle internkontrollområder.*

Innhold

[1 Innledning 1](#_Toc90497908)

[2 Virksomhetens visjon, formål og primære oppgaver 1](#_Toc90497909)

[3 Interessenter 1](#_Toc90497910)

[4 Overordnede føringer 2](#_Toc90497911)

[5 Sentrale lover, forskrifter og avtaler 2](#_Toc90497912)

[6 Andre internkontrollområder 2](#_Toc90497913)

[7 Eksisterende organisering innen informasjonssikkerhet 2](#_Toc90497914)

[8 Andre vesentlige rammevilkår og forhold 3](#_Toc90497915)

[8.1 Ekstern databehandler 3](#_Toc90497916)

[8.2 Trender rundt trusler 3](#_Toc90497917)

[8.3 Trender rundt sårbarheter 3](#_Toc90497918)

# Innledning

Dette notatet oppsummerer og klargjør rammebetingelser som kan påvirke arbeidet med styring av informasjonssikkerhet.

Notatet skal være grunnlag for de som arbeider med å utforme utkast til føringer til virksomhetsledelsen, for avdelinger og seksjoner når de involveres, og for virksomhetsledelsen selv.

Notatet er utarbeidet av arbeidsgruppen ………. og ferdigstilt dd.mm. 2016.

# Virksomhetens visjon, formål og primære oppgaver

[VIRKSOMHETEN]s visjon er ……

[VIRKSOMHETEN]s formål er å ……

De primære oppgavene fremgår av virksomhetens strategi og består av:

* Behandle og lagre økonomiske data om byggeprosjekter i [sted]
* Behandle og lagre kartdata
* Behandle og lagre persondata for innbyggerne i [sted]

# Interessenter

Våre oppgaver og informasjonsbehandling er spesielt av interesse for:

* Innbyggere
	+ Disse vil være opptatt av [tillit til oss, tjenestetilbud, kvalitet…]
* Næringsliv
	+ Effektiv saksbehandling, søknadsprosess […]
* Kommunestyret
	+ Informasjon om …
* Fagdepartement
	+ Informasjon om …
* Andre
	+ Arbeidstilsynet: Informasjon om helse, miljø og sikkerhet
	+ Kommunerevisjon: Informasjon om regnskap
	+ Nn: Informasjon om …

# Overordnede føringer

Vårt [fagdepartement/kommunestyre] har gitt følgende føringer med betydning for informasjonsbehandling og informasjonssikkerhet

* ….
* ….

# Sentrale lover, forskrifter og avtaler

Informasjonssikkerheten i [VIRKSOMHETEN] er regulert av en rekke lover og regler. Under nevnes noen av de viktigste:

* Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)
* Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
* Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
* Lov om kommuner og fylkeskommuner (kommuneloven)
* Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
* Lov om nasjonal sikkerhet (sikkerhetsloven)
* Forskrift om virksomheters arbeid med forebyggende sikkerhet (forskrift til sikkerhetsloven)
* Lov om behandling av personopplysninger (personopplysningsloven) og personvernforordningen
* Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften)

# Andre internkontrollområder

Virksomheten har i ulik grad systematisk internkontroll på følgende områder

* Virksomhetssstyring
	+ Ansvar: Internkontrollenheten i STAB
* Helse, miljø, sikkerhet (HMS)
	+ Ansvar: Personalseksjonen i ADM
* ?

# Eksisterende organisering innen informasjonssikkerhet

Informasjonssikkerhet har frem til nå i stor grad vært oppfattet som IKT-sikkerhet. Ansvaret har derfor frem til nå vært tillagt IKT-seksjonen. ……

Det eksisterer lite formell oppfølging opp mot virksomhetsledelsen.

De ulike fagavdelingene har et uklart forhold til hvilket ansvar de har.

Det er et visst samarbeid mellom IKT-seksjonen og bygningsansvarlig i ADM med hensyn til fysisk sikkerhet.

# Andre vesentlige rammevilkår og forhold

## Ekstern databehandler

Virksomheten har besluttet å kjøpe IT-tjenester fra eksterne leverandører. Dette medfører reduserte muligheter for direkte styring og kontroll av de utkontrakterte oppgavene og aktivitetene. Dette må således gjøres indirekte gjennom detaljerte leveranseavtaler, ytelsesrapporteringer fra og statusmøter med leverandørene.

Dersom tjenestene inneholder personopplysninger må det inngås databehandleravtale med leverandørene. Dette er en plikt virksomheten har etter personvernforordningen artikkel 28.

## Trender rundt trusler

I følge dokumentet «Nasjonalt digitalt risikobilde 2021» fra NSM har NSM i 2020 og 2021 opplevd en markant vekst i aktivitetsnivå i det digitale rom sammenlignet med tidligere år.

De skriver: «Antall alvorlige hendelser registrert hos NCSC i 2020 var tre ganger så mange som i 2019. Flere av disse var omfattende operasjoner hvor flere virksomheter var berørt. (…) Hendelser knyttet til krypteringsvirus øker og blir mer avanserte.»

## Trender rundt sårbarheter

Nåværende system for overvåking og hendelseshåndtering inneholder lite. Det er vanskelig å si noe om trender utover at de ansatte i liten grad ser ut til å rapportere hendelser.

Arbeidsgruppen har gjennomført uformell samtale med noen sentrale aktører for internkontroll- og sikkerhetsarbeid. Oppsummert synes det å være lite fokus rundt om i virksomheten på

* innholdet i og betydningen av systematikk i internkontrollarbeidet
* betydningen av etterlevelse av sikkerhetstiltak
* tilpasning av sikkerhetstiltak til målene de ulike enhetene skal nås, arbeidet som skal gjøres og risikoene ved brudd på konfidensialitet, integritet og tilgjengelighet

Situasjonen på konfidensialitet synes å være noe bedre enn for de to andre. Det er samtidig klare indikasjoner på at situasjonen varierer sterkt mellom ulike organisatoriske enheter.

Det synes gjennomgående å være lite bevissthet på risikoer som kan skyldes uhell og uaktsomhet.

Det kan se ut som om vi har rimelig dyktige folk på IT-drift, men tiltak de iverksetter selv og kravene til ansatte som de får besluttet, synes i stor grad å mangle kobling til de organisatoriske enhetenes situasjon, behov og risikoer. Dette kan både redusere effektiviteten mer enn nødvendig og medføre at mange ikke bryr seg om sikkerhetstiltakene, uavhengig av om de er viktige eller ikke.

Vi synes å ha lite egenkontroll på bygningsmassen, adgangskontroll mv.. Det er huseier som styrer dette. Bygningsansvarlig i ADM er med i husstyret, men signaliserer at hun gjennomgående har lite gjennomslag,