***(Teksten merka med gult her innleiingsvis er ein kommentar***

*Dette dømet er ei enkel skisse til eit notat som bør utarbeidast innleiingsvis i arbeidet med føringar for styring av informasjonssikkerheit. Innretning og omfanget på notatet må tilpassast eigenarta til verksemda og dei behov ein meiner å ha i det vidare arbeidet med føringane.*

*Ein bør spesielt vurdere om ein skal gå nærare inn på pkt. 6 «Andre internkontrollområde», sjå konkret på kva ein har frå før der, for å ta stilling til om delar av føringane kanskje bør vere felles for fleire eller alle internkontrollområde.*

Innhald

[1 Innleiing 1](#_Toc59544542)

[2 Verksemda sin visjon, føremål og primære oppgåver 1](#_Toc59544543)

[3 Interessentar 1](#_Toc59544544)

[4 Overordna føringar 2](#_Toc59544545)

[5 Sentrale lovar, forskrifter og avtalar 2](#_Toc59544546)

[6 Andre internkontrollområde 2](#_Toc59544547)

[7 Eksisterande organisering innan informasjonssikkerheit 2](#_Toc59544548)

[8 Andre vesentlege rammevilkår og tilhøve 3](#_Toc59544549)

[8.1 Ekstern databehandlar 3](#_Toc59544550)

[8.2 Trendar rundt truslar 3](#_Toc59544551)

[8.3 Trendar rundt sårbarheiter 3](#_Toc59544552)

# Innleiing

Dette notatet oppsummerer og klargjer sentrale rammevilkår som kan påverka arbeidet med styring av informasjonssikkerheit.

Notatet skal vere grunnlag for dei som arbeider med å utforme utkast til føringar til verksemdsleiinga, for avdelingar og seksjonar når dei vert involverte, og for verksemdsleiinga sjølv.

Notatet er utarbeidd av arbeidsgruppa ………. og ferdigstilt dd.mm. 2016.

# Verksemda sin visjon, føremål og primære oppgåver

[VERKSEMDA] sin visjon er ……

[VERKSEMDA] sitt føremål er å ……

Dei primære oppgåvene går fram av verksemda sin strategi og består av:

* Behandle og lagre økonomiske data om byggeprosjekt i [stad]
* Behandle og lagre kartdata
* Behandle og lagre persondata for innbyggarane i [stad]

# Interessentar

Våre oppgåver og informasjonsbehandling er spesielt av interesse for:

* Innbyggarar
  + Desse vil vere opptekne av [tillit til oss, tenestetilbod, kvalitet…]
* Næringsliv
  + Effektiv saksbehandling, søknadsprosess […]
* Kommunestyret
  + Informasjon om …
* Fagdepartement
  + Informasjon om …
* Andre
  + Arbeidstilsynet: Informasjon om helse, miljø og sikkerheit
  + Kommunerevisjon: Informasjon om regnskap
  + Nn: Informasjon om …

# Overordna føringar

Vårt [fagdepartement/kommunestyre] har gitt følgande føringar med tyding for informasjonsbehandling og informasjonssikkerheit

* ….
* ….

# Sentrale lovar, forskrifter og avtalar

Informasjonssikkerheita i [VERKSEMDA] er regulert av ei rekkje lovar og reglar. Under vert nemnt nokre av dei viktigaste:

* 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 internkontrollområde

Verksemda har i ulik grad systematisk internkontroll på følgande område

* Verksemdsstyring
  + Ansvar: Internkontrolleininga i STAB
* Helse, miljø, sikkerheit (HMS)
  + Ansvar: Personalseksjonen i ADM
* ?

# Eksisterande organisering innan informasjonssikkerheit

Informasjonssikkerheit har fram til no i stor grad vore oppfatta som IKT-sikkerheit. Ansvaret har derfor fram til no vore lagt til IKT-seksjonen. ……

Det eksisterer lite formell oppfølging opp mot verksemdsleiinga.

Dei ulike fagavdelingane har eit uklart forhold til kva ansvar dei har.

Det er eit visst samarbeid mellom IKT-seksjonen og bygningsansvarlig i ADM når det gjeld fysisk sikkerheit.

# Andre vesentlege rammevilkår og tilhøve

## Ekstern databehandlar

Verksemda har vedteke å kjøpe IT-tenester frå eksterne leverandørar. Dette medfører reduserte moglegheiter for direkte styring og kontroll av dei utkontrakterte oppgåvene og aktivitetane. Dette må derfor gjerast indirekte gjennom detaljerte leveranseavtalar, ytingsrapporteringar frå og statusmøte med leverandørane.

Dersom tenestene inneheld personopplysningar må det inngåast databehandlaravtale med leverandørane. Dette er ei plikt verksemda har etter personvernforordninga artikkel 28.

## Trendar rundt truslar

I følge dokumentet «Nasjonalt digitalt risikobilde 2021» frå NSM har NSM i 2020 og 2021 opplevd ei markant vekst i aktivitetsnivå i det digitale rom samanlikna med tidlegare år.

Dei skriv: «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.»

## Trendar rundt sårbarheiter

Noverande system for overvaking og hendingshandtering inneheld lite. Det er vanskeleg å seie noko om trendar ut over at dei tilsette i liten grad ser ut til å rapportere hendingar.

Arbeidsgruppa har gjennomført uformell samtale med nokre sentrale aktørar for internkontroll- og sikkerheitsarbeid. Oppsummert ser det ut til å vere lite fokus rundt om i verksemda på

* innhaldet i og tydinga av systematikk i internkontrollarbeidet
* tydinga av etterleving av sikkerheitstiltak
* tilpassing av sikkerheitstiltak til måla dei ulike einingane skal nå, arbeidet som skal gjerast og risikoane ved brot på konfidensialitet, integritet og tilgjengelegheit

Situasjonen på konfidensialitet ser ut til å vere noko betre enn for dei to andre. Det er samtidig klare indikasjonar på at situasjonen varierer sterkt mellom ulike organisatoriske einingar.

Det ser ut til gjennomgåande å vere lite medvit om risikoar som kan skuldast uhell og uaktsamheit.

Det kan sjå ut som om vi har rimeleg dyktige folk på IT-drift, men tiltak dei set i verk sjølv og krava til tilsette som dei får avgjort, ser i stor grad ut til å mangle kopling til dei organisatoriske einingane sin situasjon, behov og risikoar. Dette kan både redusere effektiviteten meir enn naudsynt og føre til at mange ikkje bryr seg om sikkerheitstiltaka, uavhengig av om dei er viktige eller ikkje.

Vi ser ut til å ha lite eigenkontroll på bygningsmassen, tilgangskontroll mv.. Det er huseigar som styrer dette. Bygningsansvarlig i ADM er med i husstyret, men signaliserer at ho gjennomgåande har lite gjennomslag,