



Innleiing til styringssystemet for informasjonstryggleik og personvern

Merknad: Dette dokumentet er **ei offentleg versjon/utgåve**. Intern, konfidensiell informasjon er utelaten av omsyn til informasjonstryggleiken. Difor er heller ikkje underdokumenta i styringssystemet publiserte.

Dette dokumentet er ein del av Kinn kommune sitt styringssystem for informasjonstryggleik (informasjonssikkerheit) og personvern. Det skal gi ei overordna innføring i kvifor vi har eit styringssystem, kva det inneber og korleis dokumentasjonen er strukturert og skal brukast i kommunen.

Oppsett og malar byggjer på KiNS¹ (KiNS = Foreningen Kommunal Informasjonssikkerhet) si «verktøykasse» med undervalet «KiNS styringssystem». Lokale tilpassingar er gjort for å spegle organisering, ansvar, systemportefølje og praksis i Kinn kommune.

Kvifor eit styringssystem (internkontroll)

Kinn kommune skal ha etablert styringssystem og internkontroll for informasjonstryggleik og personvern. Kravet er forankra i lov og forskrift, mellom anna:

- [eForvaltningsforskriften § 15](#): Forvaltningsorgan skal ha internkontroll for informasjonstryggleik basert på anerkjende standardar for styringssystem, kor systemet bør være integrert i verksemda sitt heilskaplege styringssystem.
- **Personvernforordninga (GDPR)**: Særleg [artikkel 24](#) (ansvar og etterleving), [artikkel 32](#) (tryggleik ved behandling) og [artikkel 33](#) (varsling av brot).
- [Kommunelova § 25-1](#): Krav om (generell) internkontroll i kommunen.

Målet med styringssystemet er å sikre at kommunen arbeider på ein systematisk og ettervisbar måte med planlegging, gjennomføring, kontroll og forbetring av informasjonstryggleik og personvern. Dette omfattar både førebygging, handtering av hendingar og kontinuerleg forbetring over tid.

¹ KiNS: Foreningen Kommunal Informasjonssikkerhet, stiftet våren 2003. KiNS er ein norsk organisasjon / foreining som arbeider for å styrkje informasjonssikkerheita i kommunar og fylkeskommunar i Noreg. Kinn kommune er medlem.



[KiNS skriv på nettsida si](#) at alle kommunar skal ha eit styringssystem for informasjonssikkerheit (og personvern) basert på ISO 27001². Eit slikt styringssystem gir mange fordelar for ein kommune:

- Etterleving av lovverket
- Styrka informasjonssikkerheit (reduserer risikoen for sikkerheitsbrot)
- Auka tillit (kommunen tek informasjonssikkerheit på alvor)
- Effektivisering (standardiserte prosessar)
- Kontinuerleg forbetring (forbetra informasjonssikkerheit over tid)

Leiingsforankring og ansvar

Styringssystemet for informasjonstryggleik og personvern **skal vera forankra i leiinga** i Kinn kommune, og inngår i kommunen sitt samla styrings- og internkontrollsystem. **Dette inneber at leiinga skal følgje opp styringssystemet og leggje til rette for etterleving og kontinuerleg forbetring.**

Leiarar på alle nivå har ansvar for å følgje opp etterleving innan sine ansvarsområde, og alle tilsette har plikt til å handle i samsvar med gjeldande policyar, retningslinjer og rutinar.

Grunnlag for dokumentasjonen

Styringssystemet byggjer på [malar frå KiNS sitt utarbeida styringssystem for informasjonstryggleik og personvern](#), og det er utarbeidd i tråd med krav og anbefalingar i relevant regelverk (rammeverk) og anerkjende standardar. Dokumentasjonen viser til og støttar mellom anna:

- **ISO/IEC 27001**: styringssystem for informasjonstryggleik
- **ISO/IEC 27002**: tiltak og kontrollar
- **ISO/IEC 27701**: personvern i styringssystemet
- **NSM sine grunnprinsipp** for IKT-sikkerheit
- **Gjeldande regelverk for digital tryggleik**, inkludert direktiv og nasjonal lovgiving som kan skjerpe krav til kommunal sektor over tid
- [Personopplysningsloven, med personvernforordninga \(GDPR, EU/EØS\)](#)
- **Nordfjordnett/IKT Nordfjord**: I nokon grad bygd vidare på det arbeidet som [Nordfjordnett](#) / IKT Nordfjord har gjort på området.
- **NIS2**: På sikt vil NIS2-direktivet bli integrert



Eventuelle krav og tiltak etter sikkerhetslova blir handterte i eigne, ikkje-offentlege styrings- og dokumentasjonsløp.

Kva er eit ISMS

ISMS er ei internasjonal forkorting for **I**nformation **S**ecurity **M**anagement **S**ystem. På nynorsk omtalar vi dette som eit styringssystem for informasjonstryggleik og personvern / **informasjonssikkerheitsstyringssystem**.

² ISO/IEC 27001 er ein internasjonal standard for styringssystem for informasjonssikkerheit (ISMS). Standarden gir retningslinjer for korleis organisasjonar kan etablere, implementere, vedlikehalde og kontinuerleg forbetre eit styringssystem for informasjonssikkerheit. Målet er å beskytte informasjonens konfidensialitet, integritet og tilgjengeligheit. ISO/IEC 27002 er òg ein standard, og gir retningslinjer for god praksis i val og bruk av sikkerheitstiltak innan informasjonssikkerheit.



Eit ISMS er eit heilskapleg rammeverk som omfattar:

- **Policyar og styrande dokument:** kva vi skal gjere og kvifor.
- **Prosedyrar, planar og malar:** korleis vi gjer det i praksis.
- **Risikovurdering og risikohandtering:** identifisere og redusere risiko.
- **Roller, ansvar og krav til etterleving:** kven gjer kva.
- **Kontroll, oppfølging og forbetring:** sikre kvalitet og kontinuerleg utvikling.

ISMS handlar ikkje berre om tekniske tryggingstiltak, men om **samspelet mellom menneske, prosessar og teknologi**.

Tryggleiksmål og tryggleiksprinsipp

Kinn kommune byggjer styringssystemet for informasjonstryggleik på etablerte tryggleiksprinsipp. Prinsippa er grunnlaget for arbeidet med informasjonstryggleik:

- **Konfidensialitet:** Informasjon skal ikkje bli kjend for uvedkomande.
- **Integritet:** Informasjon skal vere korrekt og ikkje bli endra utilsikta eller av uvedkomande.
- **Tilgjengelegheit:** Informasjon og system skal vere tilgjengelege for autoriserte personar når det trengst. Naudsynt tenestleg tilgang skal sikrast for utøving av mynde og som støtte i tenesteproduksjonen.
- **Robustheit:** System og tenester skal vere motstandsdyktige og kunne gå tilbake til normal drift etter uønskte hendingar så raskt som mogleg og innan fastsette tidsrammer.
- **Etterleving:** Informasjonsbehandling skal skje i samsvar med gjeldande policyar, retningslinjer, rutinar og regelverk (lover, forskrifter og reglement).

Kvifor ha særleg fokus på informasjonstryggleik og personvern

Kommunal sektor behandlar store mengder informasjon, inkludert personopplysningar, og leverer tenester som er kritiske for innbyggjarane. Samstundes aukar både digitalisering og trusselbiletet.

Eit godt styringssystem bidreg til:

- **Etterleving av lovverk og krav.**
- **Førebygging og reduksjon av risikoen for tryggleiksbrot og hendingar**, og redusert sannsyn for vellykka digitale angrep, mellom anna datainntrenging (digitale innbrot), datalekkasjar og at opplysningar kjem på avvegar.
- **Styrkt tillit frå innbyggjarar og tilsette.**
- **Effektivisering** gjennom standardiserte prosessar.
- **God avvikshandtering og rask gjenoppretting** ved hendingar, slik at konsekvensar blir avgrensa og normal drift raskt blir reetablert.
- **Kontinuerleg forbetring** gjennom måling, revisjon og oppfølging.

Kva betyr dette for innbyggjarar og brukarar av kommunale tenester

For innbyggjarar, tenestemottakarar og andre som kjem i kontakt med Kinn kommune, betyr dette styringssystemet at kommunen arbeider systematisk for å verne informasjon og personopplysningar mot misbruk, tap og uønskte hendingar.

Styringssystemet skal bidra til at personopplysningar blir behandla på ein trygg, føreseieleg og lovleg måte, at avvik og tryggleikshendingar blir handterte strukturert, og at kommunen kontinuerleg forbetrar praksis i takt med endringar i teknologi, tenester og trusselbiletet.



Korleis dokumenta i styringssystemet er strukturerte

Dokumenta i styringssystemet er organiserte i kategoriar (mapper) som speglar nivå og funksjon i internkontrollen:

- **0 Rettleiing:** rettleiingsdokument frå KiNS
- **1 Styrande:** policyar og styrande føringar (kva og kvifor)
- **2 Gjennomførande:** prosedyrar, planar og malar (korleis)
- **3 Kontrollerande:** kontroll, revisjon, måling, avvik og oppfølging
- **4 Diverse:** supplerande ressursar, bakgrunn, lenker og opplæring, supplert av oss

For oversikt over heile dokumentpakken har det blitt utarbeida eit dokument med tittelen «**0 Samla dokumentoversikt**», som listar dokumenta, ansvarlege (eigarar) og kven dokumenta har særleg relevans for. Dette hjelpedokumentet har ikkje blitt gjort offentleg tilgjengeleg, men i hovudsak er våre publiserte dokumentar dei same som KiNS har lagt ut malar av offentleg tilgjengeleg.

Språk, målgruppe og føresetnader

KiNS-malane vart opphavleg utarbeidde på bokmål. Kinn kommune og Nordfjordnett har omsett store delar av dokumentasjonen til nynorsk, men enkelte rettleiingar er førebels ikkje omsette.

[Språklova § 9](#) (klarspråk) understrekar at offentlege organ skal kommunisere klart og korrekt språk tilpassa målgruppa. Samstundes må vi vere merksame på at informasjonstryggleik og personvern er fagområde som inneheld tekniske og juridiske omgrep.

For å få fullt utbytte av dokumentasjonen er det ein føresetnad at lesaren har grunnleggjande forståing av IKT og kommunal systemforvaltning.

Forankring i samarbeid og leveranse (Nordfjordnett/IKT Nordfjord)

Kinn kommune er del av IKT-samarbeidet/oppgåvefelleskapet [IKT Nordfjord / Nordfjordnett](#), som er strategi- og driftseining for IKT. Ein vesentleg del av arbeidet med retningslinjer, instruksar og rettleiingar er utvikla i fellesskapet mellom Nordfjord-kommunane (Bremanger, Gloppen, Kinn, Stad og Stryn) inkludert Kinn kommune, og gjeld for kommunane i samarbeidet. I tillegg finst fagnettverk og ei eiga IKT-tryggingsgruppe som handterer felles utfordringar innan personvern og informasjonstryggleik.

Samarbeidet har mellom anna bidrege med:

- tryggingshandbok
- felles IKT-reglement
- retningslinjer for bruk av kunstig intelligens
- ulike ROS- og DPIA-arbeid

Lenkjer og referansar til tidlegare og anna arbeid er samla i eigne dokument i styringssystemet (mellom anna eige lenkedokument, ikkje gjort offentleg tilgjengeleg). Dokumentet inneheld lenkjer og informasjon om tidlegare og anna utført arbeid på personvern- og informasjonstryggleik-området i Kinn kommune og/eller i regi av IKT Nordfjord/Nordfjordnett.

Nordfjordnett har som nemnt allereie gjort ein stor jobb på området ISMS, og dei har gitt kommunane i samarbeidet tilgang til det dei har utarbeidd. Likevel må kvar kommune i samarbeidet tilpasse dokumentasjonen til sin verksemd, noko som no har blitt utført for Kinn kommune sin del.



Det er viktig å presisere at sjølv om tekniske oppgåver og delar av praktisk gjennomføring kan vere delegert til Nordfjordnett/IKT Nordfjord, **har Kinn kommune som verksemd det overordna ansvaret for informasjonstryggleik og personvern i eigen organisasjon** (og er behandlingsansvarleg, eit ansvar som ikkje kan delegerast bort).

Dokumentomfang og bruk (korleis du som lesar bør starte)

Dokumentpakka utgjer samla sett Kinn kommune sitt styringssystem for informasjonstryggleik og personvern for eigen organisasjon (om lag 80 dokument).

For effektiv intern bruk:

- Start med «**0 Samla dokumentoversikt**» for å finne relevante dokument for di rolle.
- Les deretter dei **styrande dokumenta (policyar)** som gjeld for alle tilsette og/eller di funksjon.
- Bruk **gjennomførande og kontrollerande dokument** når du skal utføre oppgåver, vurdere risiko, handtere avvik eller gjennomføre kontroll/revisjon.

Det er ikkje nødvendig å lese alle dokument frå A til Å, og ikkje alle dokument er relevante for alle tilsette.

Utfyllande dokumentasjon er tilgjengeleg i kommunen sitt **avviks- og kvalitetsstyringssystem Compilo**. Av omsyn til informasjonstryggleik er denne dokumentasjonen ikkje offentleg tilgjengeleg, utover den informasjonen som er presentert i dette dokumentet.

Operasjonalisering og etterleving

Å ha dokumenta er ikkje nok – dei må bli operasjonaliserte og etterlevde i praksis. For at styringssystemet skal ha reell effekt, må det:

- **Forankrast** i leiinga og i organisasjonen på alle nivå – frå topp til botn
- **Evaluerast** jamleg og **vidareutviklast**
- **Operasjonaliserast** gjennom rutinar, opplæring og praksis
- **Etterlevast** i det daglege arbeidet



Tal på filer og mapper tilgjengeleg internt i Kinn kommune

Kinn kommune – ISMS-filer

Mappe:	Tal på undermapper og filer:
 0 Rettleiing	7 filer, 0 mapper
 1 Styrande	35 filer, 2 mapper («Temaspesifikke policyar» og «Topp policyar»)
 2 Gjennomførande	23 filer, 0 mapper
 3 Kontrollerande	14 filer, 0 mapper
 4 Diverse	41 filer, 2 mapper
Rot-nivå (toppnivå)	2 filer («0 Innleiing» og «0 Samla dokumentoversikt»), 5 mapper

Diverse-katalogen inneheld primært perifere filer og støtte-/arbeidsmateriale, inkludert generelt underlag («KI-mat») for KI-agent på personvernområdet. Innhaldet er i hovudsak ikkje ein del av den formelle ISMS-dokumentasjonen.

Oppdatert pr. 05.01.2026, av personvernrådgjevar Bjørn Roger Rasmussen.

Personvern – kort innføring

Kinn kommune behandlar personopplysningar som ein del av lovpålagde oppgåver, tenesteyting, myndigheitsutøving og administrasjon. Behandlinga skjer i tråd med personopplysningsloven og personvernforordninga (GDPR), og byggjer på fastsett rettsleg grunnlag, hovudsakleg heimel i lov. I enkelte tilfelle blir behandling gjennomført på grunnlag av samtykke frå den registrerte.

Personvern handlar om retten til privatliv og retten til å bestemme over eigne personopplysningar. Kommunen behandlar berre nødvendige personopplysningar, og arbeider etter prinsippet om dataminimering. Behandling av særlege kategoriar av personopplysningar (sensitive personopplysningar, mellom anna helseopplysningar) krev særleg rettsleg grunnlag og skal skje med stor varsamheit.

Personvern og informasjonstryggleik heng tett saman. Informasjonstryggleik handlar om å verne all informasjon som kommunen behandlar, uavhengig av om ho inneheld personopplysningar eller ikkje. Målet er å sikre konfidensialitet, integritet og tilgjenge for informasjon og system, og å førebyggje uønskte hendingar som datainntrenging, tap av data eller driftsavbrot. Personvern handlar særskilt om vern av personopplysningar og rettane til dei registrerte. Informasjonstryggleik er ein viktig føresetnad for godt personvern, men personvern omfattar òg forhold som går utover tryggleikstiltak, til dømes behandlingsgrunnlag og dei registrerte sine rettar.

For kvar behandlingsaktivitet som omfattar personopplysningar, skal kommunen ha dokumentasjon i behandlingsprotokollar. Desse dannar grunnlaget for personvernerklæringar som gir open og forståeleg informasjon til innbyggjarar, tenestemottakarar, tilsette og andre registrerte om korleis personopplysningar blir behandla, og kva rettar dei har.

Personvern er ein integrert del av kommunen sitt styringssystem for informasjonstryggleik og personvern (ISMS). Gjennom systematisk internkontroll, risikovurderingar (ROS), databehandlar-avtalar og vurderingar av personvernkonsekvensar (DPIA der det er krav om eller behov for det), skal

kommunen sikre konfidensialitet, integritet og tilgjengelegheit for personopplysningar. Arbeidet med personvern er kontinuerleg og blir vidareutvikla i takt med endringar i system, tenester og trusselbiletet.

Meir utfyllande informasjon om personvernet i Kinn kommune er tilgjengeleg gjennom lenkjer seinare i dokumentet.

Personopplysninger:



Ordsky: Personopplysningar kan vere både direkte identifiserande (som namn og fødselsnummer) og indirekte identifiserande. Ofte må fleire opplysningar koplant saman før det er mogleg å identifisere ein person. Ordsky laaa med ChatGPT 5.2 (KI).

Ansvar

- **Dokumenteigar:** Personvernrådsgjevar IKT (tryggingsansvarleg) eig dette dokumentet.
- **Relevans:** Dokumentet er relevant for alle tilsette, leiarar og systemeigarar som kjem borti kommunal IKT-bruk og/eller behandling av informasjon og personopplysningar.
- **Ansvarsdeling:** Ein del tekniske oppgåver og praktisk gjennomføring på IKT-området er delegert til Nordfjordnett/IKT Nordfjord, men Kinn kommune har det overordna ansvaret for informasjonstryggleik og personvern.
- **Kunstig intelligens:** Kunstig intelligens (ChatGPT 5.2) er nytta til språkvask, forbetring av formuleringar og forslag til betre struktur og ordval.



Referansar

Anna relevant regelverk på området:

- [Forskrift om elektronisk kommunikasjon med og i forvaltningen \(eForvaltningsforskriften\)](#)
- [Lov om kommuner og fylkeskommuner \(kommuneloven\)](#)
- [Lov om behandling av personopplysninger \(personopplysningsloven\), med personvernforordninga \(GDPR, EU/EØS\)](#)
- [Lov om elektronisk kommunikasjon \(ekomloven\)](#)
- [Lov om nasjonal sikkerhet \(sikkerhetsloven\)](#)
- [Lov om digital sikkerhet \(digitalsikkerhetsloven\)](#), jf. NIS1-direktivet (og etter hvert NIS2-direktivet)
- [Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret \(sivilbeskyttelsesloven\)](#)
- [Lov om rett til innsyn i dokument i offentlig verksemd \(offentleglova\)](#)
- [Lov om dokumentasjon og arkiv \(arkivlova\)](#): Arkivregelverket med lov og forskrift regulerer forvaltninga av arkiv og stiller krav om utarbeiding av arkivplan som del av arkivstyringa.

Kinn kommune – personvern (lenker):

- [Personvern og "Cookies"](#)
- [Generell personvernerklæring](#)
- [Generelt om personvern og personvernerklæringar | Personvernerklæringar for særskilde/einskilde behandlingar](#)
- [Generelt om personvern – Kinn kommune \(PDF med utdrag frå lenkja over\)](#)

Endringslogg

Dokumentversjon	Endringar	Endra dato	Endra av
1.0	Oppretting av dokument.	15.12.2025	Bjørn Roger Rasmussen
1.1	Oppretting av offentlig versjon, med seinare mindre justeringar.	20.01.2026	Bjørn Roger Rasmussen