2003 20 ÅR 2023

KiNS

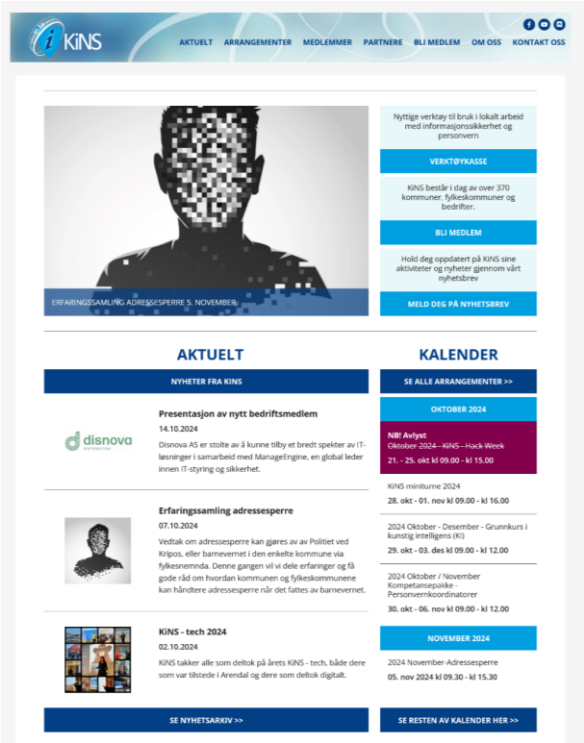
foreningen kommunal informasjonssikkerhet

Sikkerhetsdagen 2024 – Digi Rogaland

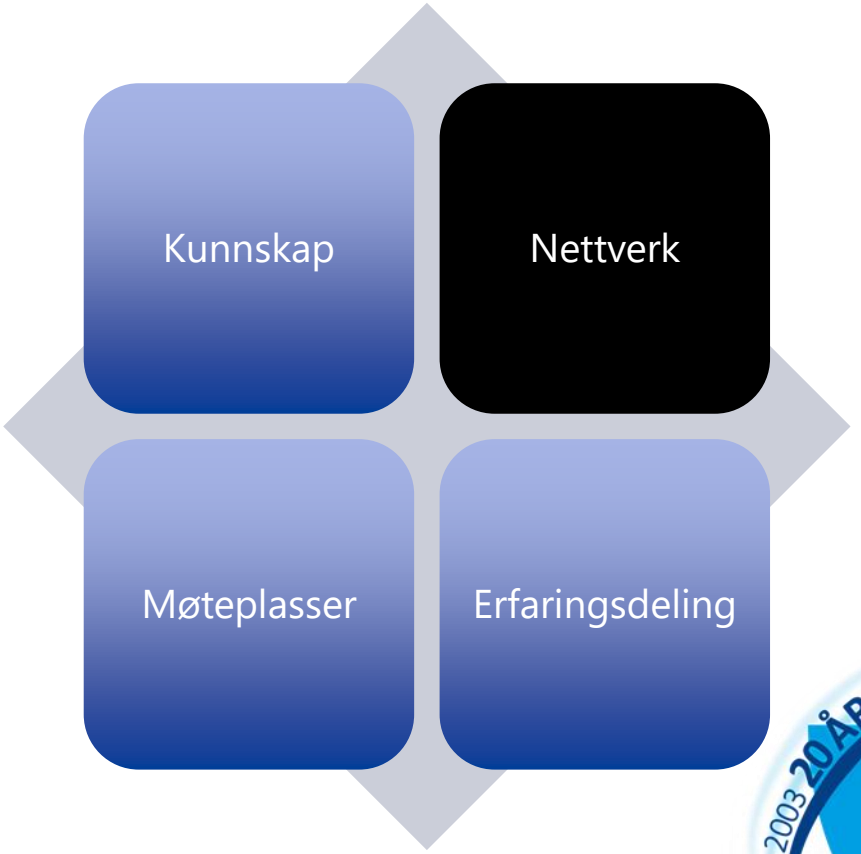
Medlems- og interesseforening

Formål:

Å bidra til å ***styrke kommuner*** og ***fylkeskommuner*** sitt arbeid med ***informasjonssikkerhet*** og ***personvern***



Nettverk – tilhørighet og knutepunkt



Erfaringsdeling

KiNS styringssystem

KiNS har på i samarbeid med Sandefjord, Horten og Ringerike kommune initiert et prosjekt for å styrke arbeidet med styringssystem for informasjonssikkerhet i kommunesektoren.

Kompetanse og opplæring

Her samler vi ressurser til bruk i opplæring og kunnskapsbygging lokalt i fylkeskommuner og kommuner.

Digital sikkerhet og beredskap

Her vil vi dele ressurser og erfaringer som kan være til hjelp for å styrke arbeidet med digital sikkerhet, informasjonssikkerhet og lokalt beredskapsarbeid i den forbindelse

Personvernkonsekvensutredning

Data Protection Impact Assessment - DPIA, eller en personvernkonsekvensutredning er en plikt etter personvernregelverket. Den skal sikre at personvernet til de som er registrert i løsningen ivaretas.

Maler for databehandleravtaler

Her deler KiNS anbefalte maler for databehandleravtale fra våre medlemmer og samarbeidspartnere.

Schrems II og leverandøroppfølging

"Sekreteriatet" for nettverk for kommunale personvernombud har kommet med forslag til tekst man kan anvende i leverandøroppfølging i lys av Schrems II dommen. KiNS tar gjerne i mot forslag til forbedringer og vil videreformidle disse til nettverk for kommunale personvernombud.

Adressesperre

Adopsjon av security.txt i norsk offentlig sektor

Dette er en ressurs delt med KiNS fra vårt bedriftsmedlem Kovert. Hensikten er å opprette en tekstfil på en webserver, som brukes til å informere om hvordan en organisasjon kan kontaktes for å rapportere sårbarheter til dem og annen relevant informasjon.

Ressurser til bruk i risiko- og sårbarhetsvurderinger

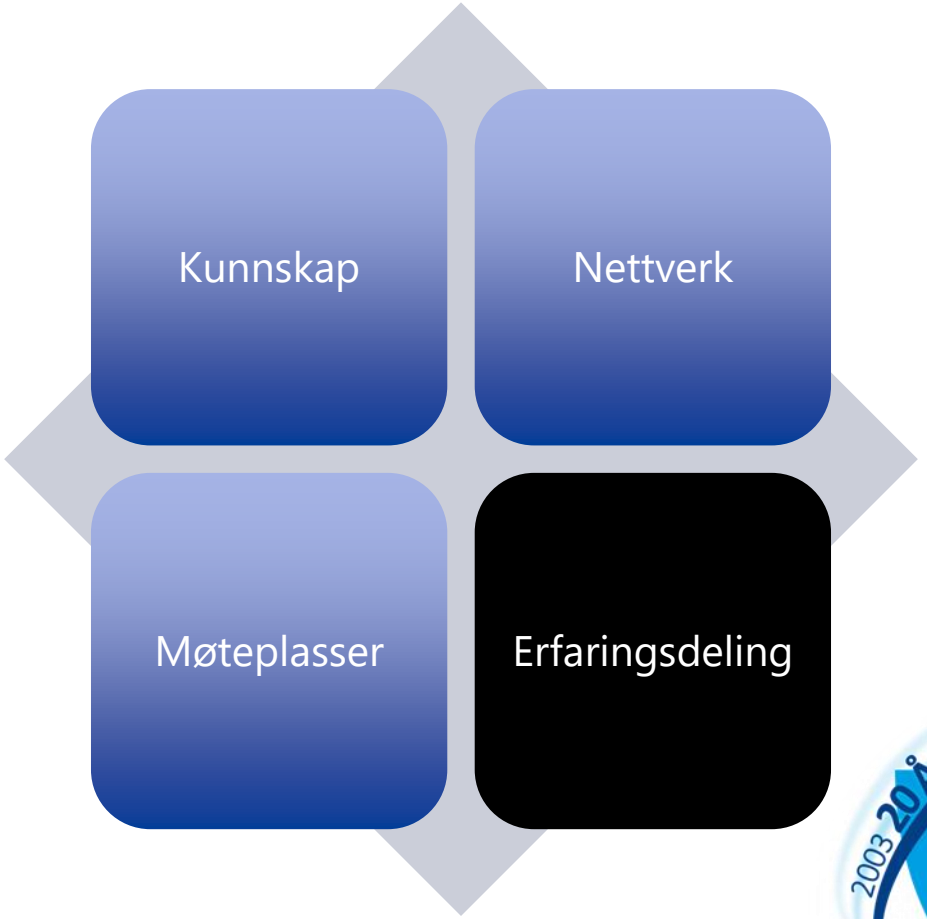
På denne siden vil vi samle maler og erfaringer fra kommuner og fylkeskommuner som vil være til i kommuner og fylkeskommuner sitt lokale arbeid med risiko- og sårbarhetsvurderinger

Verktøy for generering av sikkerhetskrav

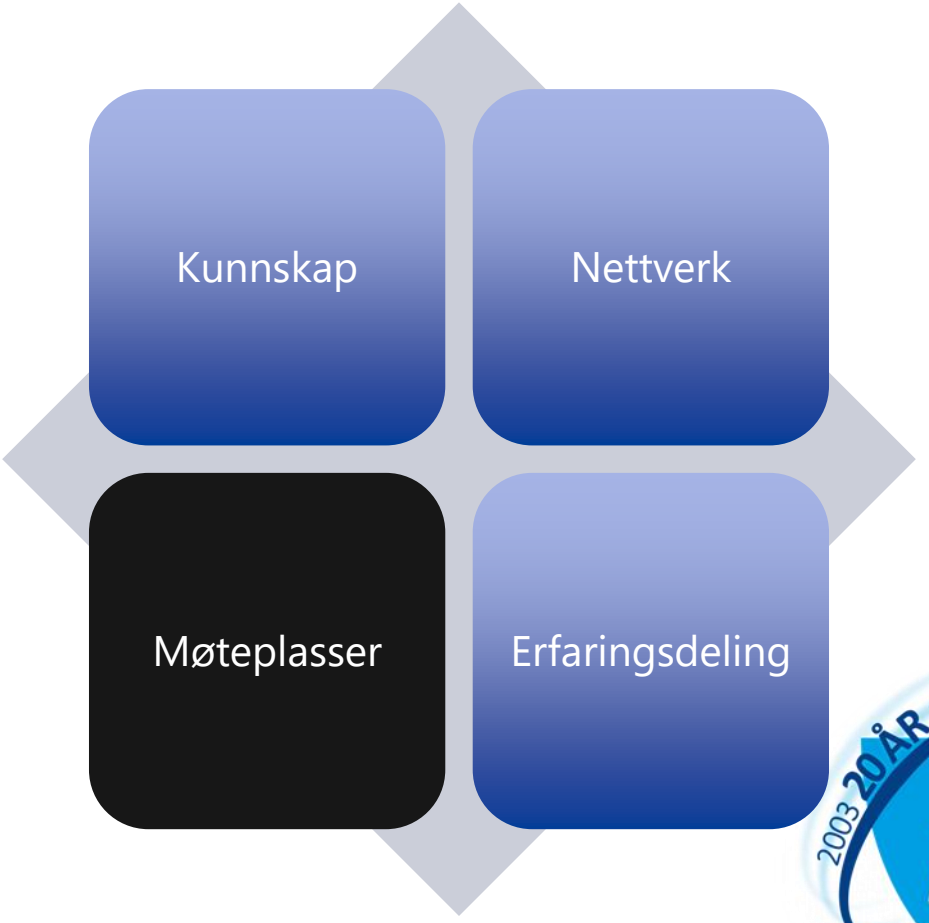
KiNS har i samarbeid med kommunale medlemmer utviklet et verktøy for å fremskaffe relevante sikkerhetskrav når det skal anskaffes digitale ressurser til kommunen.

Risikobank - risikoscenarioer og tiltak

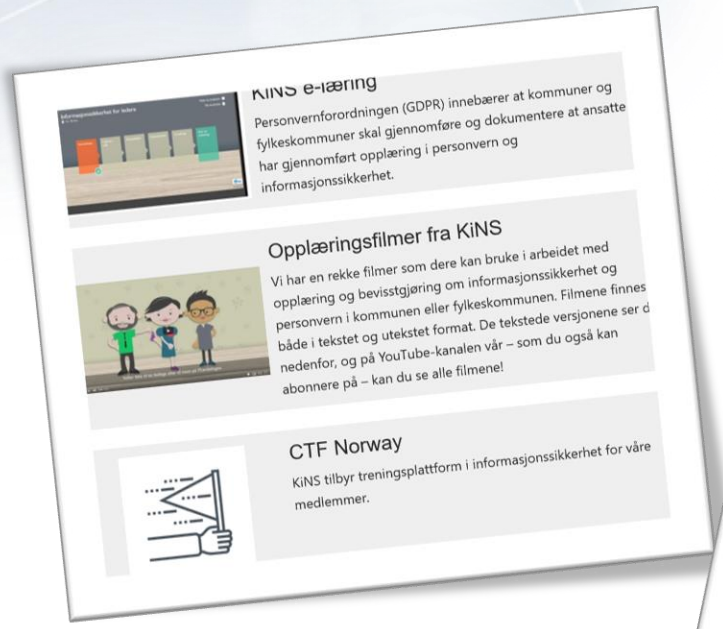
I samarbeid med kommunale medlemmer og vårt bedriftsmedlem Iconfirm har vi fått utviklet et verktøy for deling av eksempler på risikoscenarioer og tiltak som er relevante for gjennomføring av risikovurderinger og DPIA i egen organisasjon.

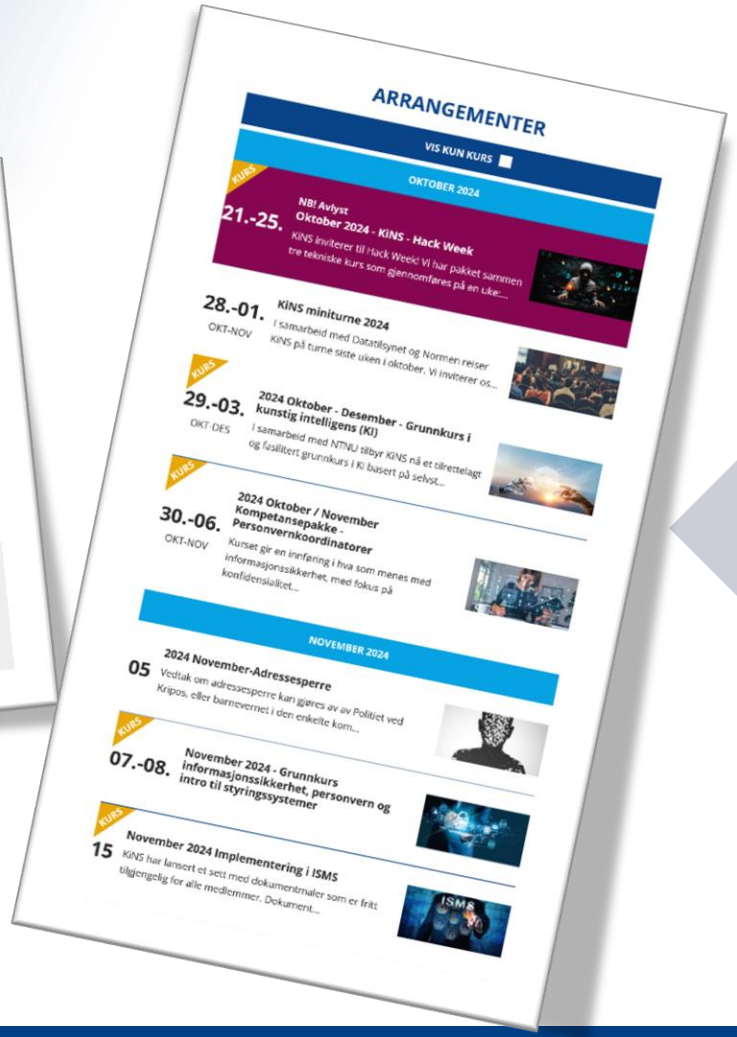


Møteplasser-konferanser, seminarer, webinarer



Kunnskap –kompetanse og opplæring





- Kunnskap
- Nettverk
- Møteplasser
- Erfaringsdeling

Systematisk tilnærming til informasjonssikkerhet og personvern – hvor skal vi begynne?

Informasjonssikkerhet handler om

- Å øke kvaliteten på leveransene og arbeidet i kommunen/FK

- God bruk av ressurser
- Sikre riktig kompetanse hos ansatte
- Bidra til innebygd informasjonssikkerhet i løsninger
- Gjøre det mulig å måle effekten av sikkerhetstiltakene
- Bidra til at informasjonssikkerheten revideres og evalueres

Personvern

- Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.
  - En menneskerettighet
  - Sikre felles goder i et demokratisk samfunn
  - Sikre demokratiet og ytringsfriheten

Hva koker det ned til?

Kommunens virksomhetsstyring

Hva koker det ned til?

Beslutningsgrunnlag

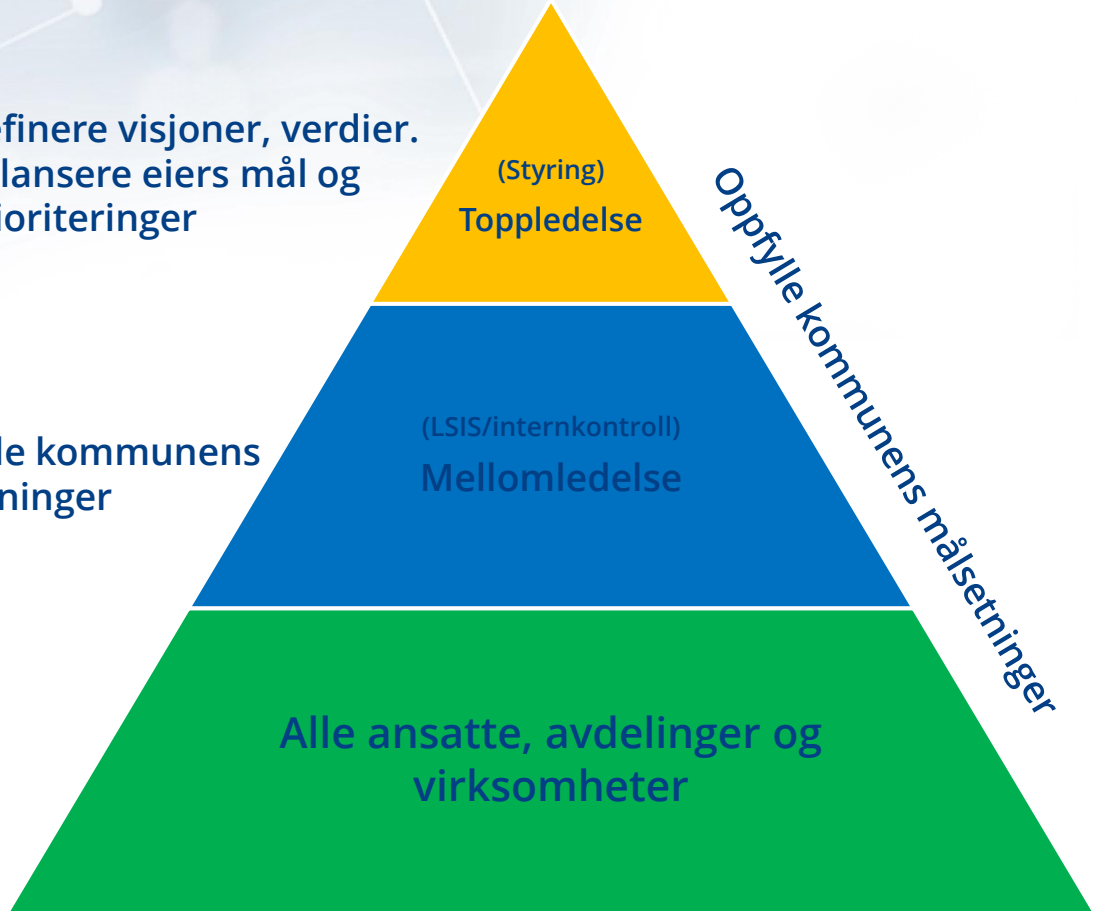
Hva koker det ned til?

Styringsinformasjon

Hvor begynner vi?

Rammene for arbeidet må defineres!

Vi begynner med toppledelsen



- Ansvaret ligger hos politisk og administrativ ledelse
- Gjennom sikkerhetsstrategien defineres rammene for resten av organisasjon
- Gjør det mulig å kunne aggregere styringsinformasjon tilbake.

KiNS styringssystem

- Et slikt styringssystem gir mange fordeler for en kommune:
  - Etterlevelse av lovverket
  - Styrket informasjonssikkerhet (reduserer risikoen for sikkerhetsbrudd)
  - Økt tillit (kommunen tar informasjonssikkerhet på alvor)
  - Effektivisering (standardiserte prosesser)
  - Kontinuerlig forbedring (forbedret informasjonssikkerhet over tid)

Dokumentene i KiNS styringsystem

Styrende del	Gjennomførende del	Kontrollerende del	Veiledning og støttedokumenter
• 2 topp policyer • 25 temaspesifikke policyer	• 8 prosedyrer • 4 planer • 3 maler • 1 skjema	• 7 prosedyrer • 3 maler • ISMS dashboard	• Mapping mot NSM grunnprinsipper • Mapping mot GDPR • Veiledning til malsettet

Eksempel på sammenheng mellom policyer og prosedyrer

Eksempel på sammenheng mellom policyer og prosedyrer

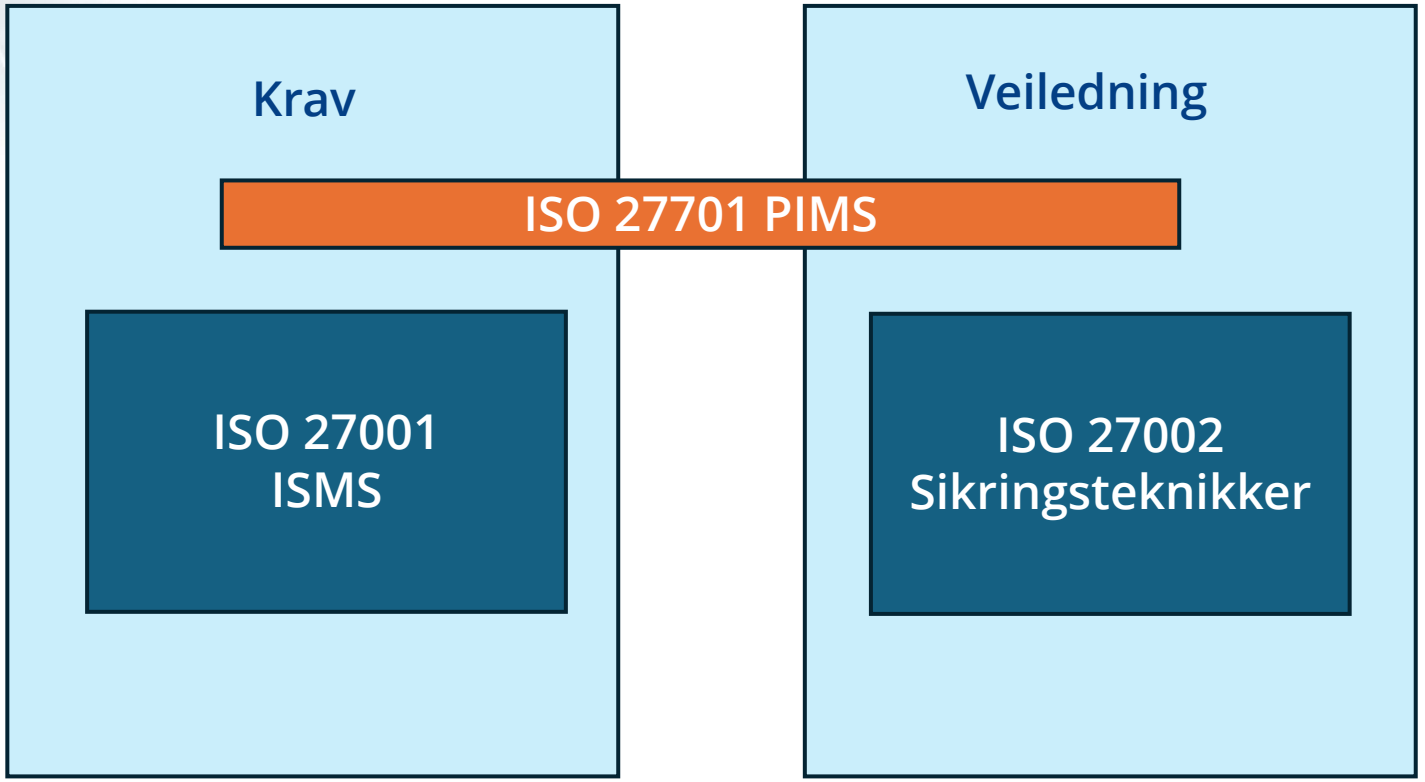
Hovedversjonene i KiNS ISMS

Versjon 1
ISO 27001 og
ISO 27002

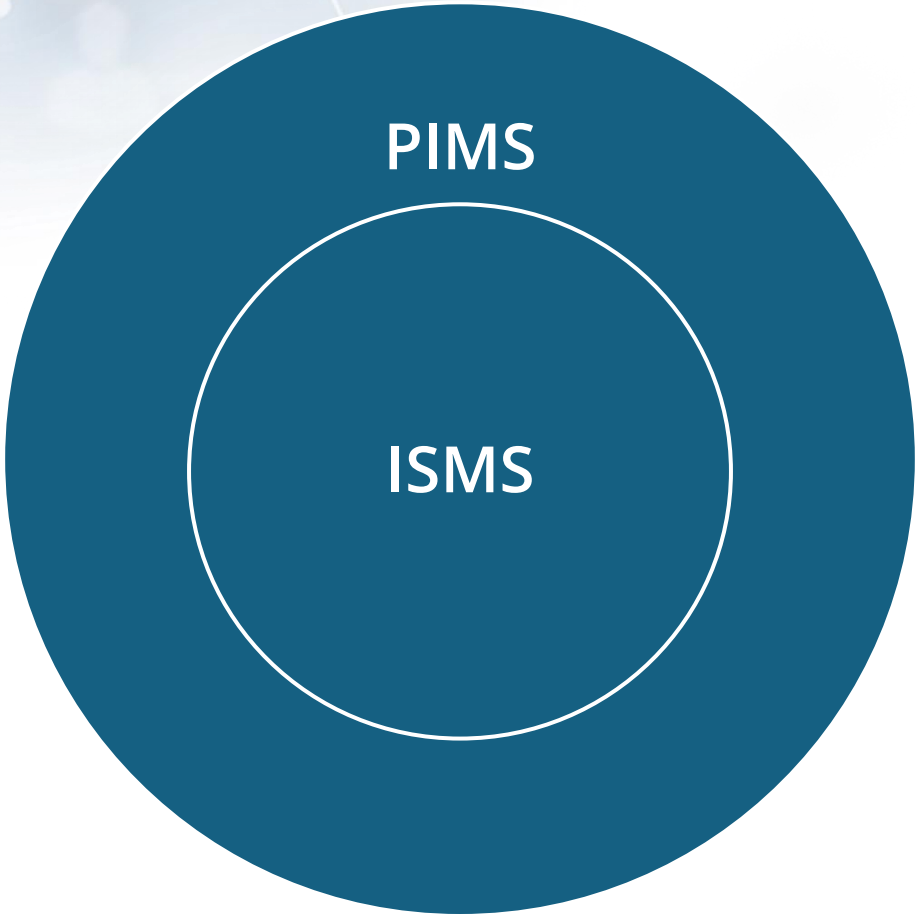
Versjon 2
NIS2-direktivet

Versjon 3
ISO 27701 og
GDPR

ISO 2700 standardene



Fra ISMS til PIMS



- ISMS – sikre virksomhetens egen informasjon
- PIMS – Sikre de registrertes personopplysninger som står utenfor selve virksomheten. De registrertes rettigheter står sterkt.

KiNS styringssystem - hva er nytt?

- **Styringssystemet er oppdatert i henhold til NIS2-direktivet:**
  - Ledelsens ansvar og governance (artikkel 20)
  - Sikkerhetskravene (artikkel 21)
  - Rapporteringsplikten (artikkel 23)

- **Styringssystemet er utvidet i henhold til ISO 27701 og GDPR:**
  - Implementert tilleggsveiledningene i ISO 27701 klausul 5, 6 og 7
  - Utvidet relevanserklæringen (SOA) i henhold til ISO 27701 Annex A
  - NB! Gjeldende ISO 27701 versjon er ikke i samsvar med gjeldende versjoner av ISO 27001 og ISO 27002. Vi må påregne noe revisjon når ny versjon av ISO 27701 blir tilgjengelig.
  - NB! Det er inkonsistenser mellom ISO 27701 og GDPR. Vi har prøvd å dekke hullene.

- **Alle dokumentene har gjennomgått mindre revisjoner.**

KiNS styringssystem

KiNS Verktøykasse

Dokumenter > General > **KiNS styringssystem**

	Navn	Endret	Endret av	Versjon
	1. Dokumenter som hører til den styrende delen av styringssystemet	6. oktober 2023	Harald Torbjørnsen	1.0
	2. Dokumenter som hører til den gjennomførende delen av styringssystemet	6. oktober 2023	Harald Torbjørnsen	1.0
	3. Dokumenter som hører til den kontrollerende delen av styringssystemet	6. oktober 2023	Harald Torbjørnsen	1.0
	Veiledningsdokumenter	6. oktober 2023	Harald Torbjørnsen	1.0

Relevans erklæringen (SOA)

- Lister opp alle 93 sikkerhetstiltak (kontrollere) i ISO 27002
- KiNS ISMS relevanserklæring er mappet mot NSM sine grunnprinsipper for IKT-sikkerhet

- Kommunen bør ta stilling til alle:
  - Er de enkelte sikkerhetstiltakene relevant for kommunen?
  - Er de enkelte sikkerhetstiltakene implementert?
  - Hvilket dokument (policy, prosedyre) omfatter de enkelte sikkerhetstiltakene?

- Hva bør ligge til grunn for å velge et sikkerhetstiltak?
  - Risikovurderinger
  - Kontraktuelle bestemmelser
  - Juridiske krav
  - Beste praksis

Relevanserklæringen (SOA) er utvidet med ISO 27701 kontrollerne

Klausul/gruppe	Kontroll	Kontrolltittel	Dokumentnavn i malsettet
teknologiske tiltak	8.31	Separasjon av utviklings-, test- og produksjonsmiljøer	
teknologiske tiltak	8.32	Endringshåndtering	
teknologiske tiltak	8.33	Testinformasjon	
teknologiske tiltak	8.34	Beskyttelse av informasjonssystemer under revisjonstesting	
betingelser for innsamling og behandling	7.2.1	Identifisere og dokumentere formål	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.2	Identifisere rettslige grunnlag	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.3	Bestemme bruk av samtykke	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.4	Inhente og lagre samtykke	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.5	Vurdering av personvernkonsekvenser	Policy for behandling av personopplysninger + prosedy
betingelser for innsamling og behandling	7.2.6	Databehandleravtale	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.7	Felles behandlingsansvarlig	Policy for behandling av personopplysninger
betingelser for innsamling og behandling	7.2.8	Behandlingsprotokoll	Policy for behandling av personopplysninger + behandl
forpliktelser ovenfor de registrerte	7.3.1	Bestemme og oppfylle forpliktelser ovenfor de registrerte	Policy for å ivareta de registrertes rettigheter
forpliktelser ovenfor de registrerte	7.3.2	Fastsette informasjon til de registrerte	Policy for å ivareta de registrertes rettigheter
forpliktelser ovenfor de registrerte	7.3.3	Informere de registrerte	Policy for å ivareta de registrertes rettigheter
forpliktelser ovenfor de registrerte	7.3.4	Mekanisme for å endre eller trekke samtykke	Policy for å ivareta de registrertes rettigheter
forpliktelser ovenfor de registrerte	7.3.5	Mekanisme for å protestere	Policy for å ivareta de registrertes rettigheter

Relevanserklæring (SOA)

Risikovurdering

De ansatte blir nettfisket, dvs at de utleverer brukernavn og passord til trusselaktører. Risiko må reduseres med tiltak.

Valg av sikringstiltak

6.3 Bevisstgjøring, utdanning og opplæring i informasjonssikkerhet

Relevant dokument

Kompetanseplan

Relevanserklæring (SOA)

Risikovurdering

Kommunens leverandører bli kompromittert og trusselaktør får tilgang til kommunen IT-systemer. Sikringstiltak er nødvendig

Valg av sikringstiltak

5.19 Informasjonssikkerhet i leverandørforhold

5.20 Håndtering av informasjonssikkerhet i leverandøravtaler

5.21 Håndtering av informasjonssikkerhet i IKT-leveransekjeden

Relevant dokument

Policy for leverandørstyring

Dokumentene har referanser til standardene og NIS2

Resultat

Lavere risiko for uautorisert tilgang til informasjon som behandles i kommunens informasjonssystemer.

Referanser

- ISO 27002:2022 5.15 «Tilgangskontroll»
- ISO 27002:2022 5.16 «Identitetshåndtering»
- ISO 27002:2022 5.18 «Tilgangsrettigheter»
- ISO 27002:2022 8.2 «Privilegerte tilgangsrettigheter»
- ISO 27002:2022 8.3 «Begrensninger på informasjonstilgang»
- ISO 27002:2022 8.5 «Sikker autentisering»
- ISO 27701:2019 6.6.2 «User access management»
- NIS2 artikkel 21 nummer 2 bokstav j «The use of multifactor or continous authentication»

3

Mapping mot NSM sine grunnprinsipper

Mapping mellom ISO 27002, KiNS styringssystem og NSM grunnprinsipper for IKT-sikkerhet

ISO-standard	Kontroll	Kontrolltittel	Dokument i KiNS ISMS	NSM grunnprinsipper for IKT-sikkerhet 2.0
ISO 27002 organisatoriske tiltak	5.1	Policyer for informasjonssikkerhet	Policy for informasjonssikkerhet	1.1.2
ISO 27002 organisatoriske tiltak	5.2	Roller og ansvar for informasjonssikkerhet	Roller og ansvar	1.1.2, 1.3.3
ISO 27002 organisatoriske tiltak	5.3	Arbeidsdeling	Roller og ansvar	
ISO 27002 organisatoriske tiltak	5.4	Lederansvar	Roller og ansvar	1.1.2
ISO 27002 organisatoriske tiltak	5.5	Kontakt med myndigheter	Prosedyre for kontakt med myndigheter	
ISO 27002 organisatoriske tiltak	5.6	Kontakt med spesielle interessegrupper	Prosedyre for kontakt med myndigheter	
ISO 27002 organisatoriske tiltak	5.7	Trusseletterretning	Prosedyre for innhenting av trusselinformasj	1.1.3, 3.1.2
ISO 27002 organisatoriske tiltak	5.8	Informasjonssikkerhet i prosjektstyring	Policy for informasjonssikkerhet i prosjekter	2.1.1, 2.1.2, 2.1.3, 2.3.3, 2.3.7, 2.3.8, 2.3.1(
ISO 27002 organisatoriske tiltak	5.9	Oversikt over informasjonsverdier og andre	Policy for styring av informasjonsverdier	1.1.5, 1.1.6, 1.2.1, 1.2.2, 1.2.3, 1.2.4
ISO 27002 organisatoriske tiltak	5.10	Akseptabel bruk av informasjonsverdier og	Sikkerhetsinstruks	
ISO 27002 organisatoriske tiltak	5.11	Retur av verdier		
ISO 27002 organisatoriske tiltak	5.12	Klassifisering av informasjon	Policy for klassifisering av informasjon	2.7.5
ISO 27002 organisatoriske tiltak	5.13	Merking av informasjon	Prosedyre for merking av informasjon	
ISO 27002 organisatoriske tiltak	5.14	Informasjonsoverføring	Policy for informasjonsoverføring	1.1.2, 2.1.4, 2.1.9, 2.5.2, 2.5.7, 2.5.8, 2.7.2,
ISO 27002 organisatoriske tiltak	5.15	Tilgangskontroll	Policy for tilgangsstyring	1.1.2, 2.6.1, 2.6.6

Mapping mot GDPR

Mapping mellom GDPR, KiNS styringssystem og ISO 27701

GDPR artikkel	Dokument i KiNS styringssystem	Referanse til ISO 27701
Kapittel 3 - den registrertes rettigheter		
12. Klar og tydelig informasjon	Policy for å ivareta de registrertes rettigheter	7.3
13. Informasjon som skal gis når personopplysninger samles inn fra den registrerte	Policy for å ivareta de registrertes rettigheter	7.3
14. Informasjon som skal gis når personopplysningene ikke er samlet inn fra den registrerte	Policy for å ivareta de registrertes rettigheter	7.3
15. Den registrertes rett til innsyn	Policy for å ivareta de registrertes rettigheter	7.3
16. Rett til retting	Policy for å ivareta de registrertes rettigheter	7.3
17. Rett til sletting («retten til å bli glemt»)	Policy for å ivareta de registrertes rettigheter	7.3
18. Rett til begrensning av behandling	Policy for å ivareta de registrertes rettigheter	-
19. Underretningsplikt om retting, sletting eller begrensning	Policy for å ivareta de registrertes rettigheter	7.3
20. Rett til dataportabilitet	Policy for å ivareta de registrertes rettigheter	7.3
21. Rett til å protestere	Policy for å ivareta de registrertes rettigheter	7.3
22. Automatiserte individuelle avgjørelser, herunder profilering	Policy for å ivareta de registrertes rettigheter	7.3
23. Begrensninger	-	-
Kapittel 4 - behandlingsansvarlig og databehandler		
24. Den behandlingsansvarliges ansvar	Policy for informasjonsikkerhet og personvern	-
25. Innebygd personvern og personvern som standardinnstilling	Policy for behandling av personopplysninger	7.4
26. Felles behandlingsansvarlige	Policy for behandling av personopplysninger	7.2

KiNS styringssystem – veien videre

- **KiNS styringssystem tar utgangspunkt i at kommunene og fylkeskommunene skal ha et styringssystem for informasjonssikkerhet som baserer seg på ISO 27001.**
  - Dokumentene er derfor utformet i henhold til relevante ISO-standarder, men omfatter for eksempel ikke alle veiledningspunktene i ISO 27002.

- **KiNS styringssystem vil oppdateres i november/desember, når ny versjon av ISO 27701 er tilgjengelig.**

- **KiNS styringssystem vil oppdateres når forskriften til digitalsikkerhetsloven er på plass, og når NIS2-direktivet blir innlemmet i loven.**

- **KiNS styringssystem er ikke ferdig – det er et levende styringssystem!**
  - Gi gjerne innspill og kommentarer til dokumentene
  - Gjenstår fortsatt noe revisjonsarbeid, så enkelte dokumenter vil bli oppdatert i løpet av juni

Abonner på endringer

- Automatisk tilsendt hvert kvartal

ABONNER PÅ ENDRINGSLOGG FOR KINS STYRINGSSYSTEM

Information Security Management System. Foto/illustrasjon: Shutterstock

KiNS Styringssystem tilbyr nå mulighet for å abonnere på nyhetsbrev med endringslogg for oppdaterte dokumenter.

REGISTRER FOR NYHETSBREV

KiNS styringssystem

Endringslogg

Antall oppdaterte dokumenter: 5

Dokumentstruktur i styringssystemet for informasjonssikkerhet

Versjon	Kommentar	Dato
3.0	Korrigert referanse til ISO 27003 annex A	18.03.2024

Policy for informasjonssikkerhet

Versjon	Kommentar	Dato
4.0	Mindre justeringer	21.03.2024

Roller og ansvar

Versjon	Kommentar	Dato
4.0	Lagt til beredskapsansvarlig. Koblet den til beredskapsplanen.	21.03.2024

Policy for tilgangsstyring

Versjon	Kommentar	Dato
4.0	Mindre språklige justeringer og referanser til NIS2.	22.03.2024

Policy for informasjonssikkerhet i leverandørforhold

Versjon	Kommentar	Dato
3.0	Presisert prinsipper om risikostyring av leverandørene. Revidert øvrig tekst.	21.03.2024

Implementering KiNS styringssystem

- Utforsk hva kommunen har på plass fra før, for eksempel i kvalitetssystemet.
- Gjenbruk det som kan gjenbrukes.
- Avklar ambisjonsnivået.
- Etabler ISMS-prosjekt dersom arbeidet er omfattende.

KiNS styringssystem - kursportefølje

Grunnkurs informasjonssikkerhet, personvern og innføring i styringssystemer

Implementering ISMS

Prosjektledelse av digitalinseringsprosjekter

VERKTØYKASSE

KiNS vil her publisere nyttige verktøy for kommuner og fylkeskommuner. Innholdet er utarbeidet av KiNS, medlemskommuner eller samarbeidspartnere. Vektøyene er utarbeidet av kompetente fagpersoner og organisasjoner. Den enkelte bruker av verktøyene må selv vurdere nytteverdien og er ansvarlig for egen utnyttelse av verktøyene.

Tilbud for KiNS medlemmer

Kommuner og fylkeskommuner som er medlem av KiNS har anledning til å bestille kurspakker og spesifiserte tjenester som kan skreddersys til din kommune/ fylkeskommune.

KiNS styringssystem

KiNS har på i samarbeid med Sandefjord, Horten og Ringerike kommune initiert et prosjekt for å styrke arbeidet med styringssystem for informasjonssikkerhet i kommunesektoren.

Kurs kun på bestilling

Hendelseshåndtering og digitale bevis

Gjennomføres digitalt. Lenke blir tilsendt påmeldte deltakere ett døgn i forkant

Sikkerhet i trådløse nettverk

Kurset tilsvarer innholdet til KiNS Hack Week WIFI: Sikkerhetstesting av trådløse nettverk og rfid

Sikkerhetstesting for kommuner og fylkeskommuner

Kurset tilsvarer innholdet til KiNS Hack Week Level 1: Grunnleggende sikekrhetstesting.

KiNS Spilløvelse

- Spilløvelse i digital hendelseshåndtering

En uforpliktende øvelse

- Vi vil simulere dramatikk og stress gjennom fiktive krevende situasjoner.
- Dette er en uforpliktende øvelse, uten eksterne konsekvenser.
- Det gis ikke karakterer og interne forhold offentliggjøres ikke.
- KiNS ønsker å få tilbakemelding på hva som kan forbedres og hvordan dette fungerer.

Hva er en spilløvelse

- Deltakere deles i:
  1. Øvelses deltakere (øvede aktører).
  2. Spilleder med bistand (utførere av motspill).

- Øvelsen er fiktiv
  - Forsøker å gjøre den så virkelig som mulig.
  - Mange av hendelsene er løselig inspirert av lokale forhold, og noen grad basert på virkelige hendelser.

Om spillet

- Under øvelsen arbeider dere i den fiktive kommunen «Skranten».
- Dere har samme rolle i Skranten som dere har i deres kommune.
- Vi har komprimert tidslinjen til hendelsen, og fokuserer på utvalgte scenarier.
- Spilledelsen forsøker å få god flyt, men vil måtte avbryte dere, komme med ny informasjon og gjøre sprang frem i tidslinjen.

Skranten kommune

Hendelser i spillet

- De formidles i presentasjonen eller av spilleder muntlig.
- Mottas på SMS med avsender «Ovelse».
- Spillkort som overleveres fra spilledelsen.
- Øvelsen gir et utsnitt av den virkelige hendelsesmengden.

KiNS spilløvelse i digital hendelseshåndtering

- *«Dette var realistisk og en god øvelse. Scenariet var håndterbart for å få til en god øvelse. Dette hadde passe progresjon og var realistisk. Øvelsen tok for seg utfordringer vi må regne med å stå i»,*
- *kommunedirektør Jon Steven Hasseldal.*

- *«Nye opplysninger som førte det inn i nye faser gjorde det realistisk og lærerikt. Vi må ta til oss innspill og forberede det vi kan så vi er klar i tilfelle noe lignende skjer»,*
- *ass. kommunedirektør Anne Mette Liavaag.*

Kurs og verktøy

KURS

29.-03.

OKT-DES

2024 Oktober - Desember - Grunnkurs i kunstig intelligens (KI)

I samarbeid med NTNU tilbyr KiNS nå et tilrettelagt og fasilitert grunnkurs i KI basert på selvst...

KURS

30.-06.

OKT-NOV

2024 Oktober / November Kompetansepakke - Personvernkoordinatorer

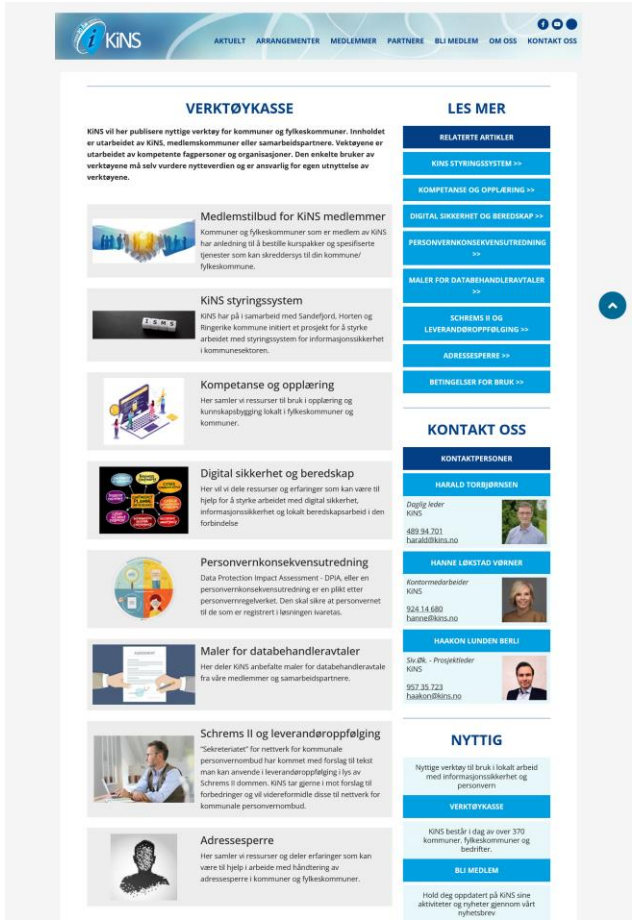
Kurset gir en innføring i hva som menes med informasjonssikkerhet, med fokus på konfidensialitet...

NOVEMBER 2024

05

2024 November-Adressesperre

Vedtak om adressesperre kan gjøres av av Politiet ved Kripos, eller barnevernet i den enkelte kom...



Takk for oppmerksomheten!

Harald Torbjørnsen
harald@kins.no