2003 20 ÅR 2023

KiNS

foreningen kommunal informasjonssikkerhet

KiNS styringssystem

KiNS styringssystem

Hva er nytt?

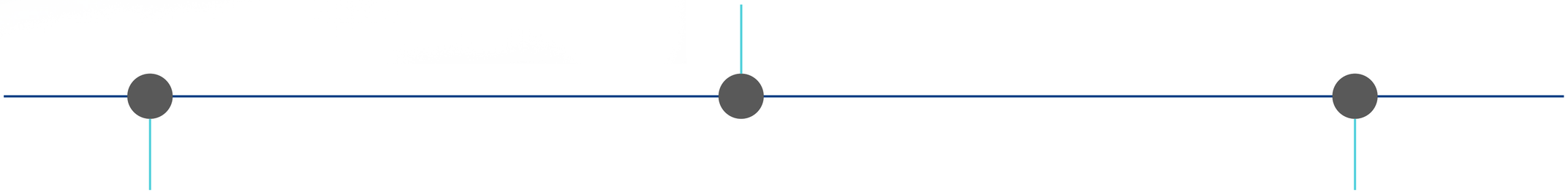
- **Styringssystemet er oppdatert i henhold til NIS2-direktivet:**
  - Ledelsens ansvar og governance (artikkel 20)
  - Sikkerhetskravene (artikkel 21)
  - Rapporteringsplikten (artikkel 23)

- **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

Hovedversjonene i KiNS ISMS



KiNS styringssystem

Dokumentene i KiNS ISMS

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

KiNS styringssystem

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

KiNS styringssystem

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

KiNS styringssystem

Mapping mellom KiNS ISMS og 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

KiNS styringssystem

Mapping mellom KiNS ISMS og 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

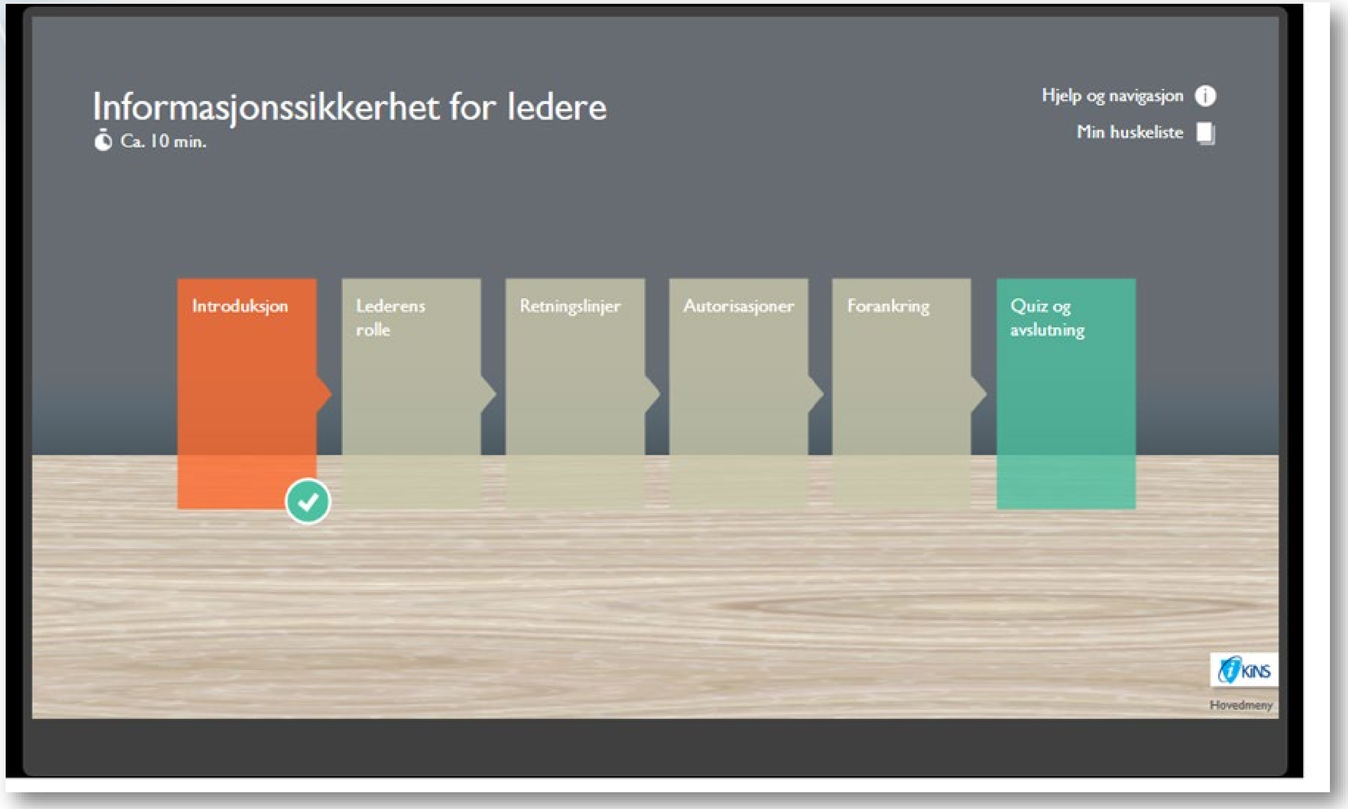
Versjon	Kommentar	Dato
4.0	Mindre språklige justeringer og referanser til NIS2.	22.03.2024

Policy for informasjonssikkerhet i leverandørforhold

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

Nyheter Verktøykassa

Kompetansepakkene revideres



KiNS Hack Week

Tre tekniske kurs på en uke!

DATO: 21. - 22. okt kl 09.00 - kl 15.00

STED: Otto Sverdrups Plass 4, 1337 Sandvika, Norge

PRIS: Se påmeldingsskjema for prisdetaljer

PÅMELDINGSFRIST: 19. aug 2024 kl 12.00

KiNS Miniturne!

KiNS, Datatilsynet og Normen kommer til deg!

DATO: 28. okt - 01. nov kl 09.00 - kl 16.00

STED: Vi kommer til deg!

PRIS: Gratis, men dere må stille med lokale og lokal markedsføring. Se mer informasjon i vedlagt dokument

PÅMELDINGSFRIST: 14. jun 2024 kl 12.00

KiNS-tech 2024

25. – 26. september i Arendal

DATO: 25. - 26. sep kl 09.00 - kl 15.00

STED: Clarion Hotel Tyholmen

PRIS: Earlybird fram til 1. juli! Se påmeldingsskjema for priser.

PÅMELDINGSFRIST: 02. sep 2024 kl 12.00

Av foreløpige navn og tematikk som er bekreftet kan vi røpe følgende:

"**Hendelseshåndtering med mer**"
- Helse- og Kommune CERT

"TBA"
- Datatilsynet

"Phishing simuleringer: Den gode, den onde og den grusomme"
- Ragnhild Sageng / Senior sikkerhetsrådgiver Tolletaten

"Fra teknikk til hacking av Fortune 1000 selskaper"
- Oddvar Moe / Principal Security Consultant TrustedSec

"2-faktor, en falsk trygghet - Fremveksten av avansert phishing"
- Jens Dale Røttereng / Sjefskonulent Atea Incident Response Team

"Når risikoen blir høy"
- Trond Sundby / CISO Bærum kommune

Standard kurs

Gjennomføres digitalt med kursholder

NOVEMBER 2024

KURS

07.-08. **November 2024 - Grunnkurs informasjonssikkerhet, personvern og intro til styringssystemer**

KURS

November 2024 Implementering i ISMS

14 KiNS har lansert et sett med dokumentmaler som er fritt tilgjengelig for alle medlemmer. Dokument...

DESEMBER 2024

KURS

05.-06. **Desember 2024 Prosjektledelse av digitaliseringsprosjekter**

Kurset tar utgangspunkt i prosjektmetodikken for offentlig sektor (prosjektveiviseren.no), herund...

KURS

29.-30. **2024 Mai - Grunnkurs informasjonssikkerhet, personvern og intro til styringssystemer - Digi Helgeland**

Antall deltakerplasser til dette grunnkurset er i sin helhet kjøpt av Digi Helgeland.

MAI 2024

KURS

24.-21. MAI-JUN **2024 Mai/juni - Grunnkurs i kunstig intelligens (KI)**

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

Takk for oppmerksomheten!

Takk til Roy Allan Hansen for produksjon og presentasjonsinnhold!

Takk til Oslo kommune, Sandefjord kommune, Kristiansand kommune, Innlandet FK, Agder FK, Buskerud FK, IKT-Agder og Digi Helgeland for innspill og kvalitetssikring.

Harald Torbjørnsen
harald@kins.no