SYKEHUSET I VESTFOLD

Dokumentstruktur i ledelsessystem for personvern og informasjonssikkerhet

Gjelder for:	Hele SiV
Dokumenttype:	Retningslinje
Sist endret:	08.02.2024

1. HENSIKT

Dette dokumentet legger rammer og føringer for hvordan dokumentene som inngår i ledelsessystem (styringssystem / ISMS – Information Security Management System) / internkontroll for personvern og informasjonssikkerhet i Sykehuset i Vestfold HF (SiV) skal struktureres.

2. ANSVAR

Hvem	Ansvar
Informasjonssikkerhetsleder Personvernombud	Begge rollene er ansvarlig for innhold og etterlevelse av dette dokumentet.

3. FREMGANGSMÅTE

3.1 Hva er et styringssystem

Styringssystemet er en samling dokumenter om hvordan sykehuset håndterer personvern og informasjonssikkerhet. Styringssystemet er bygget opp etter NS-EN ISO/IEC 27001:2023 og denne internasjonale standarden er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et styringssystem for informasjonssikkerhet. Denne typen dokumenter kalles også ISMS på engelsk (Information Security Management System).

Styringssystemet er videre en beskrivelse av vår sikkerhetsstrategi og angir de vedtatte rammene for hvordan SiV gjennom systematisk og helhetlig praksis beveger seg i takt med strategien for å nå de satte sikkerhetsmålene. Styringssystemet er en kontinuerlig forbedringsprosess og skal i tråd med SiVs kvalitetshåndbok revideres hvert andre år.

Dette dokumentet definerer også navnekonvensjoner og krav til versjonskontroll og man skal ellers følge SiVs sin prosedyre for «Utarbeidelse, revisjon, godkjenning av dokumenter EK web – Elektronisk kvalitetshåndbok – EK».
Se kapittel 5 - «Interne referanser» for nærmere detaljer om dette.

3.2 Dokumentasjon

Alle dokumenter i styringssystemet skal utformes i henhold til disse prinsippene:

- Alle dokumenter skal dokumenteres og lagres i Elektronisk kvalitetshåndbok (EK)
- Alle dokumenter skal være lesbare for alle ansatte
- Alle dokumenter skal være merket med at de tilhører SiV, det finnes også dokumenter i regionale bruksvilkår som forvaltes av Sykehuspartner (SP) og disse vil det henvises til
- Dokumenttittel skal være iht SiVs prosedyre som vist til i kapittel 5 – «Interne referanser»

3.3 Overordnet struktur av dokumentene i styringssystemet

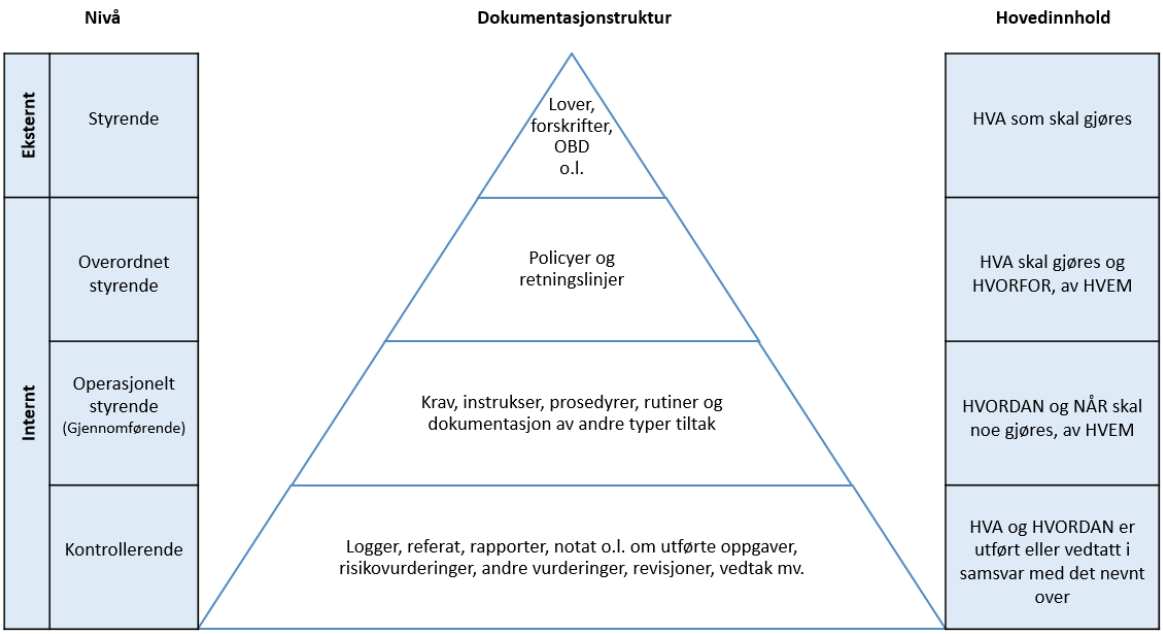
Uavhengig av om man kaller det ledelsessystem, internkontroll eller styringssystem/ISMS, så består det av tre deler som dekker de *organisatoriske*, de *menneskelige* (personellrelaterte), de *fysiske* og de *teknologiske* tiltaksområder iht. ISO 27001:2023 Tillegg A og 27002:2022.

Dokumentene i styringssystemet deles opp i tre deler; den ***styrende*** delen, den ***gjennomførende*** delen og den ***kontrollerende*** delen.

- Den **styrende** delen består hovedsakelig av retningslinjer (omtales som policy i ISO vokabularet). Mål og strategi og Organisering av personvern og informasjonssikkerhet er noen av de overordnede retningslinjen som legger rammer og føringer for hele styringssystemet. I tillegg finnes det et sett med temaspesifikk retningslinjer. Felles er at retningslinjene angir mål, prinsipper og regler som skal følges. Retningslinjene angir derfor *hva* og *hvorfor* noe skal gjøres. Styringssystemet eies av Virksomhetsstyringsavdelingen i SiV.

- Den **gjennomførende** delen består i all hovedsak prosedyrer. Disse dokumentene utledes ofte av retningslinjene, og angir *hvordan* noe skal gjøres. Prosedyrene revideres oftere enn retningslinjene.

- Den **kontrollerende** delen består av andre dokumenter, noen i form av også prosedyrer (LGG, avvik til Datatilsynet), referater (LGG), internrevisjon m.m. Disse dokumentene angir også *hvordan* noe skal gjøres.



Figur 1

3.4 Dokumentstruktur

Struktur og innhold i retningslinjene skal i utgangspunktet følge av NS-EN ISO/IEC 27000:2020, og er strukturert i henhold til NS-ISO/IEC 27003:2017 Annex A. Det innebærer at retningslinjer har følgende struktur:

- Introduksjon (innledning og formål)
- Omfang (hvor policyen gjelder)
- Målsettinger (sikkerhetsmålene for policyen)
- Prinsipper (regler som skal følges)
- Ansvar (hvem som er ansvarlig for å sikre at prinsippene følges)
- Resultat (hva er resultatet av at policyen etterleves)

Prosedyrer, planer og andre dokumenter kan ha andre strukturer.

EK er i utgangspunktet ikke bygget enhetlig etter ISO. SiVs sin prosedyre for «Utarbeidelse, revisjon, godkjenning av dokumenter EK web – Elektronisk kvalitetshåndbok – EK» skal derfor følges. Se kapittel 5 - «Interne referanser» for nærmere detaljer om dette.

4. GENERELT

5. INTERNE REFERANSER

1.1.8.2.15	Utarbeidelse, revisjon, godkjenning av dokumenter EK web. Elektronisk kvalitetshåndbok - EK

6. EKSTERNE REFERANSER

Ledelsessystemer for informasjonssikkerhet
NS-EN ISO/IEC 27000:2020
NS-EN ISO/IEC 27001:2023 7.5 «Dokumentert informasjon»
NS-EN ISO/IEC 27003:2017 Annex A

7. VEDLEGG