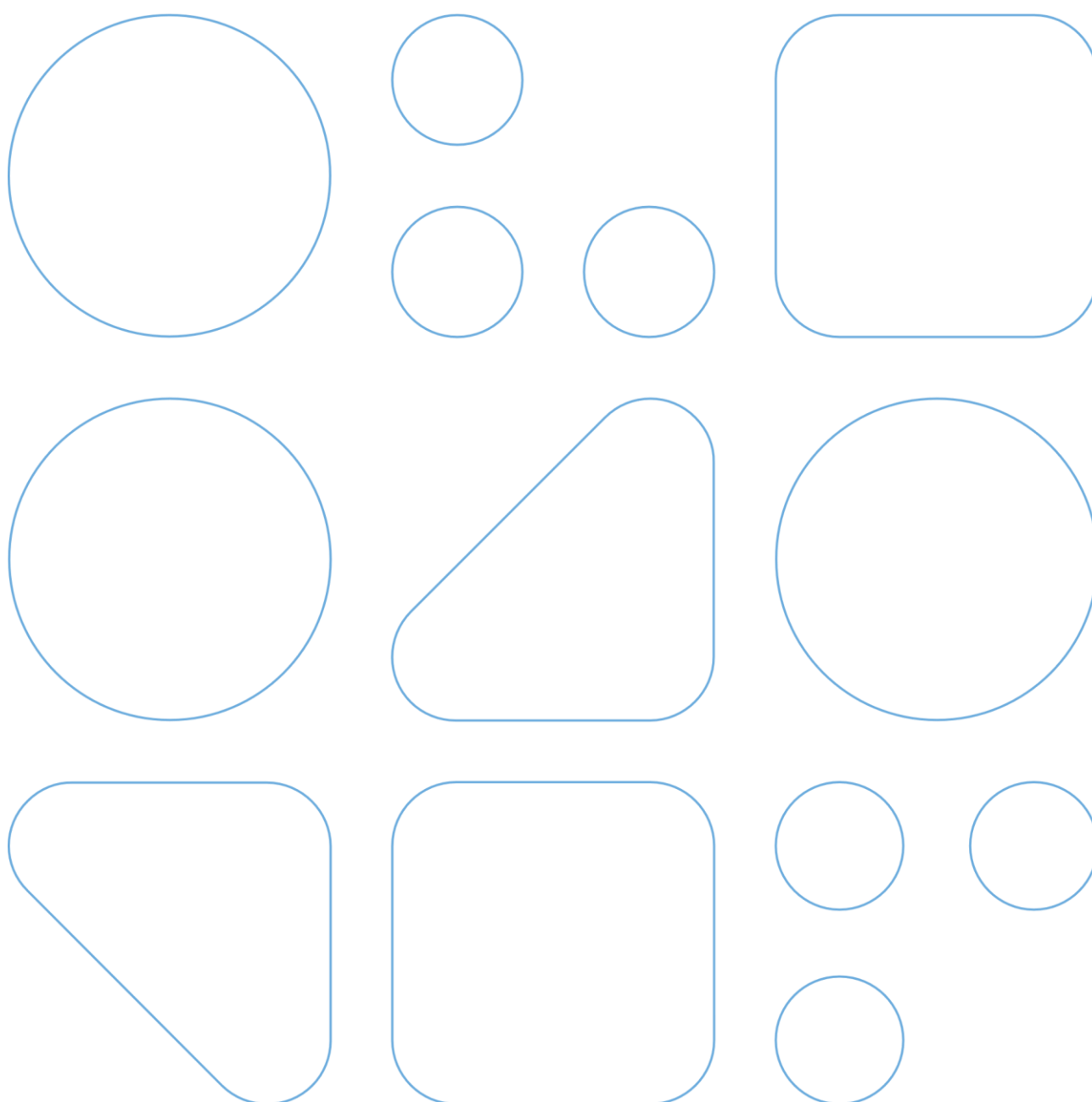


# Årsrapport

## Enhet for informasjonssikkerhet 2024

25.03.2025



# Innhold

|                                                   |    |
|---------------------------------------------------|----|
| Innhold.....                                      | 1  |
| Oppsummering.....                                 | 2  |
| 1. Innledning.....                                | 3  |
| 2. Ansatte og organisering .....                  | 3  |
| 3. Virksomhetsstyring 2024 .....                  | 5  |
| 4. Ledelsessystem for informasjonssikkerhet ..... | 7  |
| 5. Opplæring og bevisstgjøring.....               | 10 |
| 6. Kunstig intelligens .....                      | 11 |
| 7. Andre aktiviteter .....                        | 11 |
| 8. Konferanser og kursdeltakelse .....            | 12 |

## Oppsummering

Årsrapport for enhet for informasjonssikkerhet 2024 gir en oversikt over enhetens aktiviteter og prestasjoner gjennom året. Rapporten er ment for ansatte på Akershus universitetssykehus HF (Ahus) og i Helse Sør-Øst (HSØ) som ønsker innsikt i hvordan informasjonssikkerhetsarbeidet er organisert på Ahus og hva enheten har jobbet med i 2024. I 2023 ble informasjonssikkerhetsressursene omorganisert på Ahus, med en ny leder som startet i november. Enheten består nå av fire årsverk, og en ny rådgiver begynner i februar 2025.

I 2024 ble det gjennomført flere aktiviteter, blant annet arbeid med å forbedre tiltaksoppfølgingen etter risiko- og sårbarhetsvurderinger og forbedring av prosedyrer og dokumenter i ledelsessystemet for informasjonssikkerhet. Det har blitt utformet tiltakskort og prosedyre for håndtering av informasjonssikkerhetshendelser og jobbet tett med Konsernrevisjonen i forbindelse med et veiledningsoppdrag innen IKT-sikkerhet. Videre har enheten gjennomført to kontroller og håndtert 310 avvik, hvorav 67 ble meldt til Datatilsynet.

Oktober 2024 arrangerte enheten sikkerhetsmåneden for syvende år på rad med temaet "Våre digitale verdier". Aktivitetene inkluderte fagdag, spørrekonkurranse og informasjonsstands. Enheten har også jobbet med kunstig intelligens (KI) og er involvert i Ahus Innovasjonssenter for KI (AI<sup>2</sup>) som ble etablert høsten 2024.

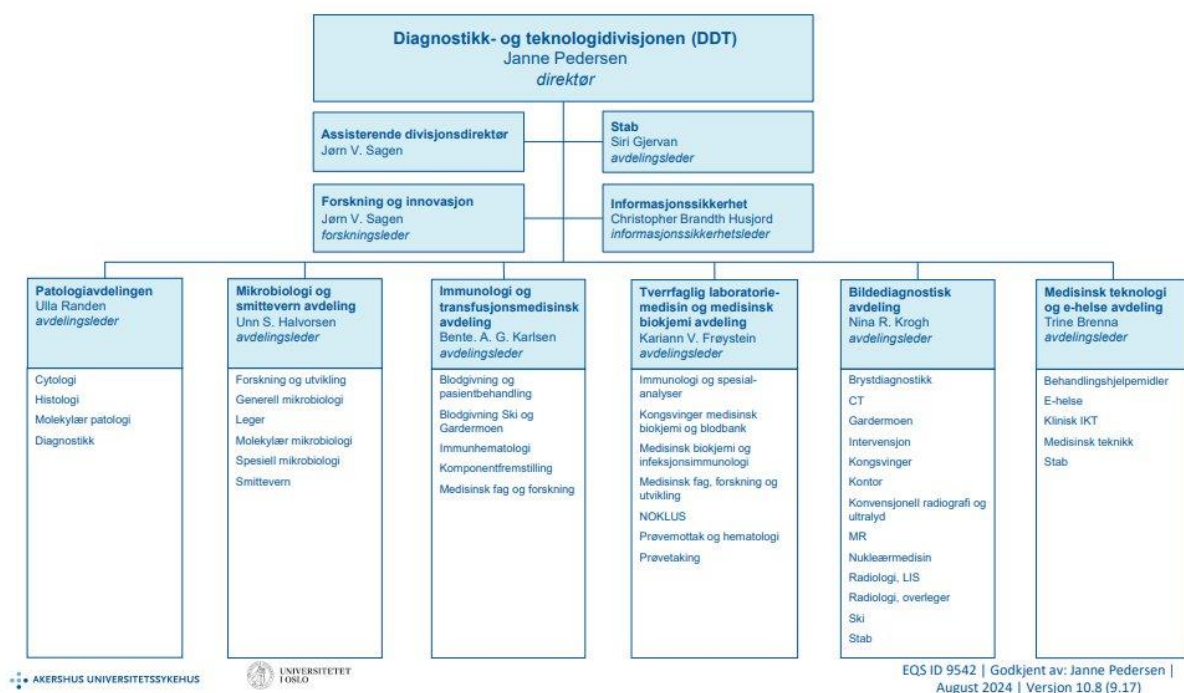
*Utkastet til oppsummeringen er generert av Copilot og tilpasset av enhet for informasjonssikkerhet.*

## 1. Innledning

Formålet med årsrapporten er å gi en oversikt over hva enhet for informasjonssikkerhet har arbeidet med og levert i løpet av 2024.<sup>1</sup> Det rapporteres overordnet på gjennomførte aktiviteter i løpet av året. Årsrapporten, sammen med tertialrapporteringen til HSØ, erstatter tilstandsrapporten som har blitt utformet årlig. Målgruppen for årsrapporten er ansatte på Akershus universitetssykehus HF (Ahus) og i Helse Sør-Øst (HSØ) som har interesse av å få innblikk i hvordan arbeidet med informasjonssikkerhet er organisert på Ahus og hva enheten har jobbet med.

## 2. Ansatte og organisering

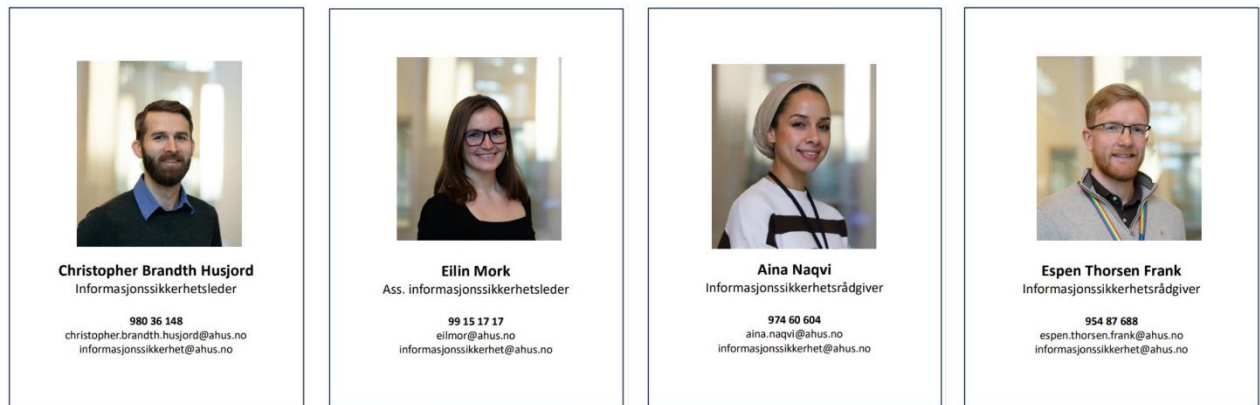
I 2023 ble det foretatt en omorganisering av informasjonssikkerhets-ressursene på Ahus. Frem til da var informasjonssikkerhetsleder ansatt i foretakssekretariatet og informasjonssikkerhetsrådgivere i staben til avdeling for medisinsk teknologi og e-helse, i diagnostikk og teknologidivisjonen. I august 2023 ble informasjonssikkerhetsleder og informasjonssikkerhetsrådgivere flyttet til en egen enhet under direktør i diagnostikk og teknologidivisjonen.



Figur 1: Enhet for informasjonssikkerhet er plassert rett under direktør for DDT

<sup>1</sup> I utgangspunktet er rapporten ment for å oppsummere året 2024. Siden vi ikke utarbeidet rapport i 2023, inngår også aktiviteter fra andre 2. halvår av 2023 i rapporten.

Ny informasjonssikkerhetsleder startet 1. november 2023 og funksjonen assisterende informasjonssikkerhetsleder ble opprettet 1. september 2023. Sammen med to informasjonssikkerhetsrådgivere har det vært fire årsverk i enhet for informasjonssikkerhet siden høsten 2023. I februar 2025 startet en ny informasjonssikkerhetsrådgiver i enheten, da det har vært et behov grunnet økte aktiviteter innen kunstig intelligens i forbindelse med etablering av Ahus Innovasjonssenter for KI (AI<sup>2</sup>).



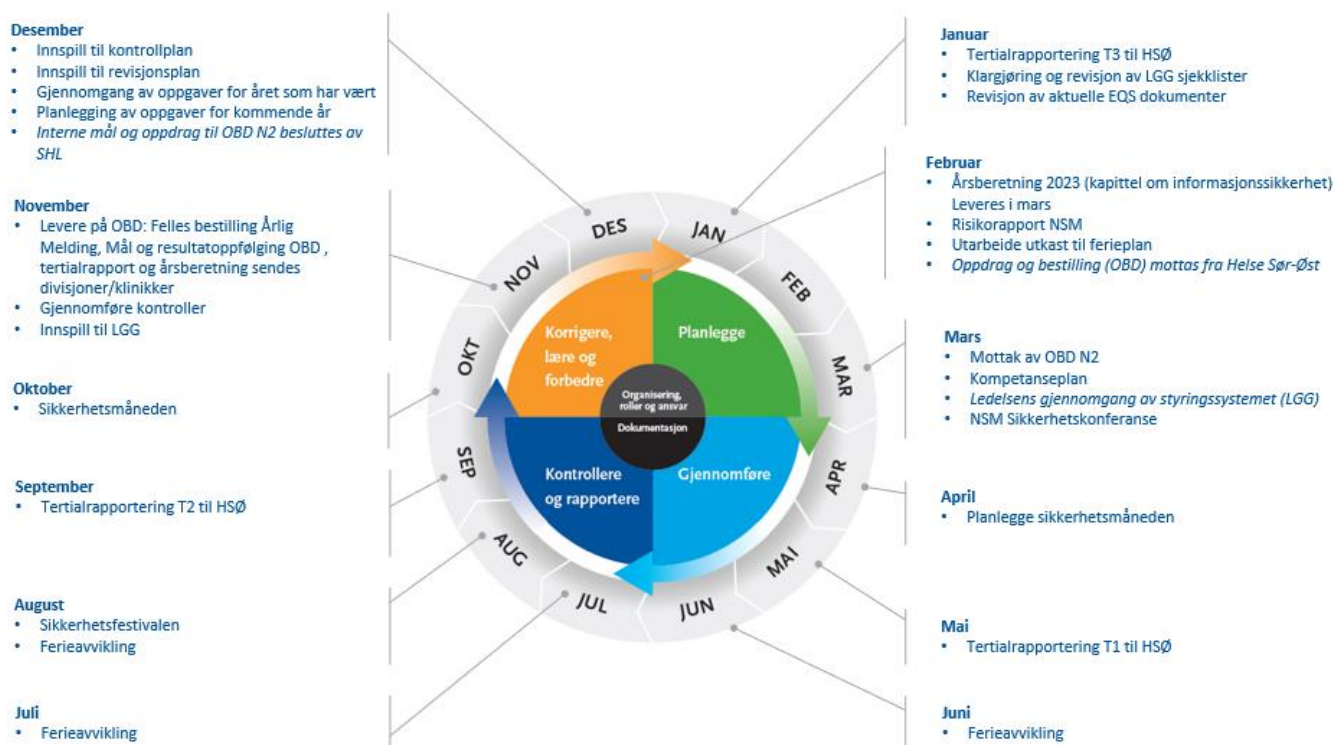
Figur 2: Ansatte per 31.12.2024

## 3. Virksomhetsstyring 2024

### Årshjul

Enheten utarbeider årlig et årshjul som benyttes for å planlegge for viktige aktiviteter. Årshjulet belyser faste aktiviteter for enheten, i tillegg til spesifikke aktiviteter som skjer for inneværende år. I denne rapporten vil flere av aktivitetene i årshjulet beskrives.

### Årshjul for Informasjonssikkerhet 2024



Figur 3: Årshjul for informasjonssikkerhet 2024

## Strategi

Enhet for informasjonssikkerhet og personvernombud har en felles strategi for internkontrollområdet som gjelder for perioden 2022-2025.



Figur 4: De seks strategiske satsningsområdene i strategi for personvern og informasjonssikkerhet 2022-2025

Enhet for informasjonssikkerhet har sammen med personvernombudet diskutert behovet for å videreføre en egen strategi for internkontrollområdet etter 2025. Vi har besluttet å ikke utforme en ny strategi, på bakgrunn av følgende forhold:

- HSØ har et overordnet, styrende dokument, *Mål og strategi for informasjonssikkerhet i Helse Sør-Øst*, som beskriver overordnede prinsipper for styring og organisering av arbeidet med informasjonssikkerhet i helseforetakene i regionen.<sup>2</sup>
- Vi mener at informasjonssikkerhet og personvern skal bidra til å understøtte virksomhetens overordnede mål slik de er dokumentert i Ahus' *Utviklingsplan 2040*.<sup>3</sup>

Vi kommer heller til å bruke *Utviklingsplan 2040* og aktuelle delplaner, som delplan 8, og *Teknologistrategien*, som de strategisk styrende dokumentene for arbeidet med informasjonssikkerhet og personvern, innenfor de rammene som settes i *Mål og strategi for informasjonssikkerhet i Helse Sør-Øst*.

<sup>2</sup> [Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF](#)

<sup>3</sup> [https://hsorhf.sharepoint.com/sites/intranett-ahus/temasider/Documents/Utviklingsplan%202040/Ahus\\_Utviklingsplan\\_2040.pdf](https://hsorhf.sharepoint.com/sites/intranett-ahus/temasider/Documents/Utviklingsplan%202040/Ahus_Utviklingsplan_2040.pdf)

## Handlingsplan

Ahus har et overordnet styringssystem, Orden i eget Ahus, som består av seks internkontrollområder: generell, kvalitet og pasientsikkerhet, HMS og ytre miljø, personvern/informasjonsikkerhet, forskning, og mattrygghet. I løpet av 2. halvår 2024 har enheten samarbeidet med de øvrige internkontrollområdene i virksomheten for å få på plass en felles handlingsplan for internkontrollområdene.<sup>4</sup>

Enhet for informasjonssikkerhet og foretakssekretariatet med personvernombud har samarbeidet om mål og tiltak for vårt internkontrollområde. Tidligere handlingsplan for internkontrollområdet, *Regional handlingsplan for informasjonssikkerhet og Utviklingsplan 2040* har vært sentrale drivere for de mål og tiltak som er foreslått.

HSØ har en årlig handlingsplan for informasjonssikkerhet, utformet av det regionale helseforetaket, som også gjelder for Ahus.

## 4. Ledelsessystem for informasjonssikkerhet

Ahus følger det regionale ledelsessystemet for informasjonssikkerhet slik det er vedtatt av Regionalt Sikkerhetsfaglig Råd (RSR) i HSØ. Dette ledelsessystemet er basert på ISO 27001 og består av regionale og lokale dokumenter, samt prosesser. Nedenfor er en beskrivelse av de viktigste aktivitetene som er utført i 2024, for å forbedre ledelsessystemet til virksomheten.

### Risikovurderingsprosess: digitale verktøy for tiltaksoppfølging

Ahus har ikke hatt et egnet verktøy for å følge opp risiko og tiltak knyttet til våre IT-systemer. Det ble derfor gjennomført en utprøving av det digitale risikohåndteringsverktøyet Diri fra Q1 2024 til Q3 2024. Diri var et bedre alternativ en daværende løsning ved bruk av excel, men mangel på importeringsfunksjonalitet resulterte i mye manuelt merarbeid for de systemansvarlige. Utprøvingen av Diri ble derfor avvirket samme år.

I Q4 2024 startet enheten en planleggingsfase med foretaksrevisjonen for å ta i bruk EQS sin handlingsplan og risikomodul for samme formål. Dette er i tråd med mål 2 i handlingsplan for internkontrollområdene for 2025-2027, om at risikomodulen i EQS skal benyttes for å gjennomføre og følge opp risikovurderinger. Med tanke på at EQS er godt kjent hos de ansatte og et verktøy som allerede ivaretar en rekke funksjoner for Ahus, forventer vi at denne handlingsplanen og risikomodulen vil være et enklere verktøy å bruke, og dermed styrke arbeidet med å følge opp informasjonssikkerhetsrisikoer og -tiltak. Ettersom at EQS er godt kjent hos de ansatte og et verktøy som allerede ivaretar en rekke funksjoner for Ahus, forventer vi at denne handlingsplanen og

---

<sup>4</sup> Sykehusledelsen besluttet i desember 2022 at det skulle jobbes videre med områdene for å få én felles handlingsplan og forenkle implementeringen og oppfølgingen, jf. sak 345/22 «Samordne mål og handlingsplaner for internkontrollområdene med Ahus OBD og mål og resultatoppfølging.»



risikomodulen vil være et enklere verktøy å bruke, og dermed styrke arbeidet med å følge opp informasjonssikkerhetsrisikoer og -tiltak.

## Prosedyrer og dokumenter i EQS

Dokumentene og prosedyrene i det regionale ledelsessystemet ligger på Sykehuspartner sine hjemmesider, og har blitt gjort tilgjengelig for Ahus gjennom lenker i egne EQS-prosedyrer. Det har vært en utfordring å holde lenkene oppdatert i EQS, da de blir utdaterte når prosedyrene oppdateres på Sykehuspartner sine hjemmesider.

Det ble derfor startet et arbeid med å samle alle relevante regionale prosedyrer i ett felles EQS-dokument med lenke til Sykehuspartners hjemmeside, i stedet for den respektive prosedyren. De EQS-prosedyrene som blir erstattet av det nye EQS-dokumentet vil bli faset ut. Januar 2025 ble den nye prosedyren (ID 46161) publisert i EQS: "Ahus - Informasjonssikkerhet: oversikt prosedyrer".

Det ble også startet en gjennomgang av alle informasjonssikkerhetsprosedyrer i EQS og etablering av nye dokumentkategorier. Arbeidet med nye dokumentkategorier ledes av foretaksrevisjonen. Gjennomgangen og ibruktakelse av de nye kategoriene ble ikke ferdigstilt i 2024 og videreføres derfor til 2025.

## Tiltakskort

Vi har i 2024 utarbeidet tiltakskort og prosedyre for håndtering av informasjonssikkerhetshendelser. Tiltakskortet skal gi veiledning til rollen "vaktansvarlig informasjonssikkerhet" og prosedyren for håndtering av informasjonssikkerhetshendelser gir en oversikt og en overordnet oppskrift på hvordan hendelser skal håndteres.

## Kontroller og revisjoner

### Kontroller

I løpet av 4. kvartal 2024 har det blitt gjennomført 2 kontroller innen informasjonssikkerhet:

1. Lagring av personopplysninger på felles lagringsområde (K:\)
2. Tilgangsstyring og krav til brukerautentisering på Medisinsk teknisk utstyr (MTU)

### Revisjoner

Det har ikke vært gjennomført revisjoner innen informasjonssikkerhet for 2024.

## Statistikk

### Risiko- og sårbarhetsvurderinger

Enhet for informasjonssikkerhet har mottatt totalt 63 nye ROS fra Sykehuspartner i løpet av 2024.<sup>5</sup> Det gjelder 22 lokale<sup>6</sup> og 41 regionale<sup>7</sup> risikovurderinger.

Risikovurderingene blir utarbeidet fra Sykehuspartner og deretter gjennomgått og akseptert på Ahus. Risikovurderingene omfatter alt fra vurderinger av journalsystemer, oppdatering av tjenester, infrastruktur og nytt medisinteknisk utstyr.

Nedenfor er en visuell oversikt som viser hvor mange ROS vi har mottatt per måned.

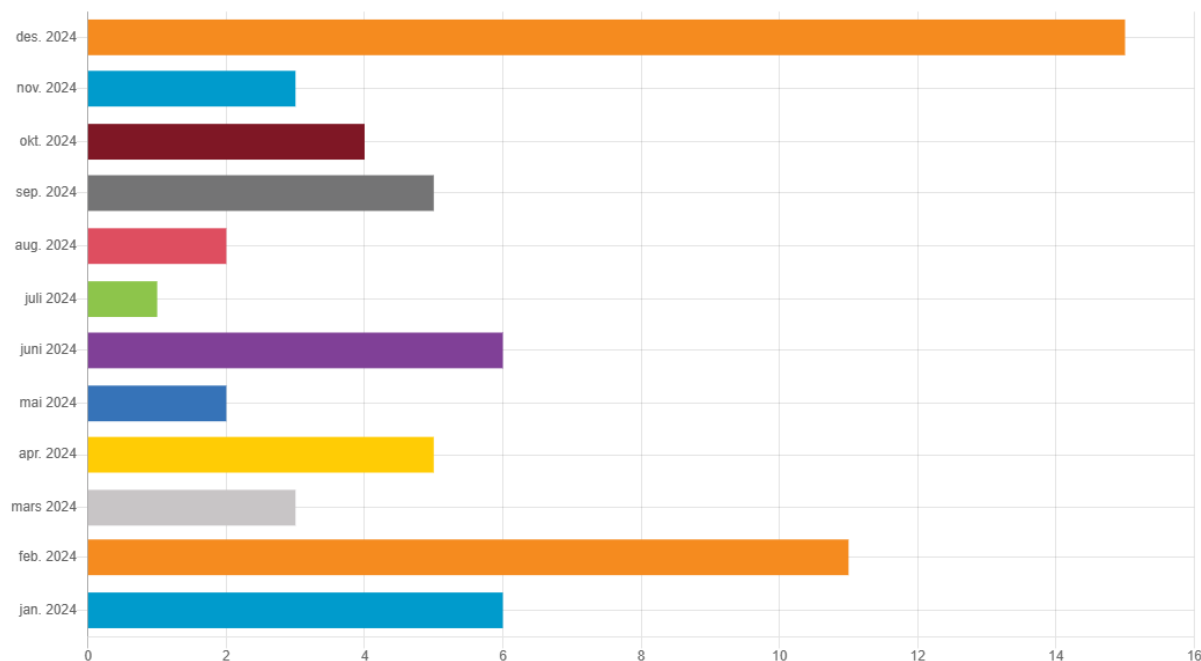


Figure 5: Antall nye ROS per måned

Risikobildet for ROS mottatt i 2024, viser at vi i løpet av 2024 har mottatt 12 tjenester med gul restrisiko eller høyere etter gjennomførte tiltak.<sup>8</sup>

### Avvik

I 2024 ble det rapportert totalt 310 avvik innen informasjonssikkerhet og personvern. Av disse ble 67 avvik meldt videre til Datatilsynet, ettersom hendelsene utgjorde en moderat eller høy risiko for de registrertes personvern. Omtrent 75% av alle rapporterte avvik var knyttet til personopplysninger

<sup>5</sup> Statistikken er basert på hvor mange nye saker som er opprettet i P360 i 2024.

<sup>6</sup> Risikovurderinger for en egen lokal tjeneste som er unik for AHUS.

<sup>7</sup> Risikovurdering for en regional tjeneste, hvor flere HF benytter tjenesten.

<sup>8</sup> Basert på gjennomgang av risikonotater i P360.

på avveie og inkluderte blant annet feilsendt pasientinformasjon og funn av pasientlister på interne områder.

## 5. Opplæring og bevisstgjøring

### Sikkerhetsmåneden

Ahus markerte sikkerhetsmåneden for 7. år på rad i oktober 2024. Tema for sikkerhetsmåneden 2024 var "Våre digitale verdier". Måneden ble markert med ulike aktiviteter, som fagdag i auditoriet (og Teams) med eksterne og interne foredragsholdere – et Cybershow av Rune Carlsen var stor suksess, spørrekonkurranse, informasjonsstands og informasjon delt på MittAhus og plakater.

Nytt av 2024 var at planlegging og gjennomføring i sin helhet ble ivaretatt av enhet for informasjonssikkerhet. Tidligere år har en gruppe bestående av representanter fra alle divisjoner (Programkomitéen) planlagt sikkerhetsmåneden, under ledelse av informasjonssikkerhetsleder. På grunn av økt bemanning og ressurser hos informasjonssikkerhet, ble det foreslått at ansvaret for planlegging og gjennomføring av sikkerhetsmåneden ivaretas av informasjonssikkerhet. Programkomitéen har fungert som ressursgruppe for innspill til tema og distribusjon av informasjon og materiell.

### Micro learning

I 2024 ble Ahus kontaktet av to leverandører, SoSafe og XtraMile, som tilbyr opplæring- og bevisstgjørings-tjenester innen informasjonssikkerhet. Etter flere møter med SoSafe ble det klart at deres tjeneste ikke er egnet for Ahus da deres plattform ikke kan integreres med Læringsportalen.

XtraMile sin plattform tilbyr APIer som muliggjør SSO og integrasjon med Læringsportalen, i tillegg til gode muligheter for å utforme kurs og opplæringsmateriale tilpasset lokale Ahus-behov. Videre prosess for å vurdere om det er aktuelt å ta i bruk XtraMile fortsetter i 2025.

### Presentasjoner og innlegg

Vi har i løpet av 2024 holdt flere interne og eksterne presentasjoner. Blant annet kan nevnes at vi har holdt presentasjon for Stavanger Universitetssykehus og brukerutvalget på Ahus om vårt arbeid med informasjonssikkerhet.

I forbindelse med arbeidet med kunstig intelligens (se kapittel 6) har assisterende informasjonssikkerhetsleder holdt flere eksterne presentasjoner og innlegg:

- Innleder på Normkonferansen om KI og risiko, 22. november 2023 (Normen)
- Webinar 12. desember 2023, med reprise 16. januar 2024 (Kvalitet og Risiko Norge)
- Presentasjon for KI-gruppen i det regionale helseforetaket (RHF), 14. desember 2023
- Presentasjon for Forsvarsmateriell, 14. mars 2024
- Innlegg på konferansen Kvalitet og Risikodagene 2024, 6. juni 2024 (Kvalitet og Risiko Norge)

- Presentasjon for IT-ledere i NAV, 10. juni 2024
- Innlegg på seminaret En fremtid med kunstig intelligens, 15. mai 2024 (Standard Norge)

## 6. Kunstig intelligens

### Ledelsessystem for KI basert på ISO 42001

Assisterende informasjonssikkerhetsleder har siden 2023 ledet arbeidet med å integrere et ledelsessystem og internkontroll for kunstig intelligens i Orden i eget Ahus. Arbeidet er basert på ledelsessystemstandarden ISO/IEC 42001 Artificial Intelligence Management System. Noen av de sentrale leveransene i dette arbeidet i 2024 var en retningslinje for bruk av generativ KI (EQS id 44868) og Ahus' policy for kunstig intelligens (EQS id 45330 og 45332). Policyen angir at det faglige ansvaret for kunstig intelligens er lagt til internkontrollområdet informasjonssikkerhet.

### Ahus innovasjonssenter for KI (AI<sup>2</sup>)

Høsten 2024 ble Ahus Innovasjonssenter for KI (AI<sup>2</sup>)<sup>9</sup> etablert. Formålet med senteret er å samle ressurser og kompetanse innen kunstig intelligens for å bidra til økt forskning, innovasjon og bruk av kunstig intelligens på Ahus. Senteret leverer to overordnede kapabiliteter: forskning og utvikling, og governance, risk and compliance (GRC). Assisterende informasjonssikkerhetsleder er ansvarlig for sistnevnte. Senteret består i tillegg av ressurser fra medisinsk teknologi og e-helse, analyseavdelingen og diagnostikk og teknologidivisjonen. Ahus innovasjonssenter for KI kan nås på [ai@ahus.no](mailto:ai@ahus.no).

Sommeren 2024 ble fagområdet kunstig intelligens (KI) lagt til internkontrollområdet informasjonssikkerhet. Assisterende informasjonssikkerhetsleder har hatt ansvaret for dette fagområdet, og har siden høsten 2024 jobbet mesteparten av tiden for det nyetablerte senteret.

### KI-dag

Mandag 9. desember arrangerte AI<sup>2</sup> en KI-dag for alle ansatte på Ahus. Fagdagen fant sted i auditoriet på Nordbyhagen og strømmet på Teams. Opptak av dagen er tilgjengelig på MittAhus. Formålet med dagen var å vise frem de ulike aktivitetene og initiativene innen KI på Ahus, samt å lansere åpningen av Ahus Innovasjonssenter for KI.

## 7. Andre aktiviteter

---

<sup>9</sup> På engelsk: Ahus Innovation Center for AI, forkortet AI<sup>2</sup>

## Konsernrevisjonen: Kartlegging av NSM's grunnprinsipper

I 2024 gjennomførte Konsernrevisjonen (HSØ) et veiledningsoppdrag (til forskjell fra revisjonsoppdrag) innen IKT-sikkerhet ved alle helseforetakene i regionen. Formålet med oppdraget var å kartlegge helseforetakenes modenhet i implementering av Nasjonal sikkerhetsmyndighet<sup>10</sup> (NSM) sine grunnprinsipper, og vurdere om de nåværende prosessene dekker hvert av disse grunnprinsippene.

Kartleggingen viste at helseforetakene har lav modenhet innen lokalt forvaltede IKT-tjenester, noe som var forventet av Konsernrevisjonen. Videre arbeid vil fokusere på å identifisere tiltak som kan bidra til å øke Ahus' modenhet i implementeringen av NSMs grunnprinsipper.

## Datatilsynet: Tilsyn vedrørende lagringsområder

I mai mottok vi et vedtak om pålegg om gjennomgang på våre lagringsrutiner utenfor journalsystemene fra Datatilsynet. Informasjonssikkerhet svarte ut en oversikt over hvilke lagringsområder sykehuset har og hvilke typer informasjon som kan lagres på de ulike områdene. Det ble også belyst utførte og planlagte tiltak i 2024, som blant annet at vi skulle gjennomføre kontroll av lagringsområdene. Datatilsynet avsluttet saken 30.10 og la til grunn at kontrollen ble fulgt opp på en tilfredsstillende måte.

## Spørreundersøkelse digital sikkerhetskultur

Siden 2022 har HSØ målt sikkerhetskulturen i foretaksgruppen gjennom spørreundersøkelsen "Kartlegging av digital sikkerhetskultur". Undersøkelsen har vært et nyttig verktøy for Ahus, ved at den gir innsikt i medarbeidernes oppfatninger og holdninger til digital sikkerhetskultur.

I 2024 ble det sendt 8427 invitasjoner, med totalt 1172 besvarelser. Dette tilsvarer en svarprosent på 14 %, og er en økning på 3,6 prosentpoeng sammenlignet med 2023. For å styrke deltakelsen ytterligere, er gjennomføring av undersøkelsen nå inkludert i Handlingsplan for informasjonssikkerhet og personvern (2025-2027).

# 8. Konferanser og kursdeltakelse

## Sikkerhetsfestivalen

August 2024 deltok alle fire i enhet for informasjonssikkerhet på Sikkerhetsfestivalen som avholdes i Lillehammer over tre dager. Festivalen er en av de største arenaene for informasjonssikkerhet i Norge og samler 1400 deltakere fra alle sektorer og bransjer. Festivalens program spres over flere parallelle spor, og assisterende informasjonssikkerhetsleder holdt et innlegg på helsesporet om ansvarlig bruk av kunstig intelligens i helsesektoren.

---

<sup>10</sup> [Nasjonal sikkerhetsmyndighet](#)

## Revisjonskurs

Våren 2024 deltok en informasjonssikkerhetsrådgiver på kurs i internrevisjon og revisjonslederkurs, i regi av Foretaksrevisjonen. Dette er en del av arbeidet med å bistå foretaket i gjennomføringen av systemrevisjoner innen informasjonssikkerhet.

## Standard Norge

Ahus inngikk avtale med Standard Norge om å holde kurs i standarden ISO 42001 AI Management System for helsesektoren. Assisterende informasjonssikkerhetsleder utformet og holdt heldagskurs standarden i september 2024.

Akershus universitetssykehus HF

Besøksadresse: Sykehusveien 25, Lørenskog  
Postadresse: Postboks 1000, 1478 Lørenskog  
Telefon: 67 96 00 00  
Epost: [postmottak@ahus.no](mailto:postmottak@ahus.no)

