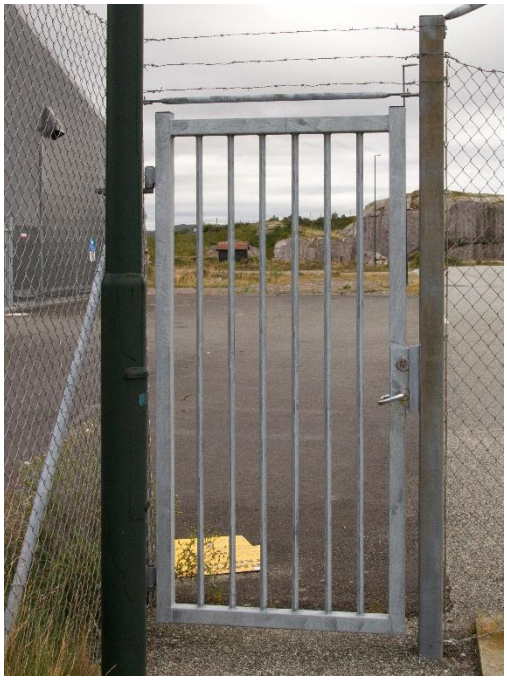
RAPPORT – RETTIGHETSSTYRING, AUTENTISERING OG AUTORISASJON, NORSK DIGITAL HAVNEINFRASTRUKTUR



SAMMENDRAG

I prosjektet Norsk digital havneinfrastruktur, i arbeidspakke 4 – Standardisering, er det lagt en aktivitet med tema Rettighetsstyring, autentisering og autorisasjon. I aktiviteten er havnedataene fra Kartverket sine havnedataprosjekt fra 2020 og 2021 sentrale. Målsetningen har vært å kartlegge brukerbehov i forhold til sikkerhet og tilgangskontroll for havnedata.

Det ble satt sammen en arbeidsgruppe, for å jobbe med dette temaet. Arbeidsgruppa har jobbet med aktuelle temaer i flere digitale workshops. Resultatene fra disse er beskrevet i denne rapporten. Rapporten vil danne grunnlag for videre arbeid i andre arbeidspakker i prosjektet Norsk digital havneinfrastruktur. Den gir også overordnede anbefalinger for veien videre.

Arbeidsgruppe – Rettighetsstyring og autorisasjon

Emne: Rettighetsstyring, autentisering og autorisasjon

Dato: 11.03.2022

Leder av arbeidsgruppa: Maléne Peterson, Norkart

Bidragsytere: **Kartverket:** Sigbjørn Wik og Niels Torger Granum. **Kystverket:** John Morten Klingsheim. **Forsvaret:** Ulrik Samdahl Melhuus. **Grieg Connect**: Dag Erik Henriksen, Anne Cecilie Rueness. **Oslo havn**: Ole Sebastian Lunde. **Arendal havn**: Gordon Fuglestad. **Bergen havn**: Stein Garmannslund, Lasse Dale. **Kristiansand havn**: Stein Roger Bjørheim. **Norkart:** Maléne Peterson.

Deltakere på temamøte Akutt beredskap i havn: **Salten brann IKS**: Øyvind Nygaard. **Nordmøre interkommunale brann- og redningstjeneste**: Jarl Arne Aspen. **110-nødsentralen**: Stian Jørgensen.

Kvalitetskontroll: Matilde Skår, Kartverket.

Bilder: Forsidebilde fra Sirevåg havn, Foto: Matilde Skår. Bilder fra RITS-øvelse: Stein Roger Bjørheim.

INNHOLD

1. BAKGRUNN OG FORVENTNINGER

Rettighetsstyring, sikkerhet og tilgangskontroll er temaer som er aktuelle både i Havnedataprosjektene i regi av Kartverket og nå også i prosjektet Norsk digital havneinfrastruktur.

I Norsk digital havninfrastruktur i arbeidspakke 4 – Standardisering, er det lagt en aktivitet med tema Rettighetsstyring, autentisering og autorisasjon. I aktiviteten er havnedataene sentrale, og det er derfor viktig å ha et forhold til Havnedata 2020 og Havnedata 2021-prosjektene til Kartverket. I havnedataprosjektene er det blitt utarbeidet en datamodell for havnedata og en registreringsinstruks for kartleggingen av dataene. I Havnedata 2.0 – modellen stilles det krav til hvilke egenskaper som er obligatoriske og valgfrie, samt hvilket kvalitetskrav som gjelder for objektene. Havnedataene tas i bruk inn i havnesystemet som utvikles av Grieg Connect.

I Havnedata 2021-prosjektet ble det ved kartlegging av brukerbehov rettet søkelys mot to tema, som også er aktuelle ift. rettighetsstyring – begge deler handler om sensitive data. Hva som er eller skal betraktes som sensitive data i havnene, vil være sentralt inn i aktiviteten.

- **Sensitive data - behandling og retningslinjer**: Tilgang til sensitive data må kunne styres. En må identifisere hvordan dataene kan håndteres på en forsvarlig måte og se på hvordan de som har behov for data f.eks. i beredskapssammenheng kan få det uten at det går utover sikkerheten.
- **Sensitive data – midlertidig lagring av farlig gods**: Ift. farlig gods vil det være viktig å kunne styre hvem som skal ha rettighet til å vite hvor det farlige godset ligger lagret.

1.1 Oppsummering – mandat

Målsetning: Arbeidsgruppa har i oppgave å kartlegge brukerbehov i forhold til sikkerhet og tilgangskontroll for havnedata. Det settes søkelys på objekter som ligger i havnedata 2.0. Gruppa ser på temaer som er aktuelle for rettighetsstyring og autorisasjon i digitale arbeidsmøter. Innspill og diskusjoner i arbeidsmøtene vil gi et godt grunnlag for å beskrive brukerbehovene tematisk. Ved behov inviteres det inn deltakere utenfor arbeidsgruppa.

Deltakere i arbeidsgruppa: Havnerepresentanter fra Arendal havn, Bergen havn, Kristiansand havn og Oslo havn, Kartverket, Grieg Connect, Forsvaret, Kystverket.

Deltakere utover arbeidsgruppa i temamøte – akutt beredskap i havn: Salten brann IKS, 110-nødsentralen.

Aktiviteten ledes av Maléne Peterson, Norkart.

Leveranse: Det skal utarbeides en rapport fra arbeidsgruppa, som vil danne grunnlag for videre arbeid i andre arbeidspakker i prosjektet Norsk digital havneinfrastruktur. Rapporten vil også gi overordnede anbefalinger for hvordan havnedataene bør gjøre tilgjengelig fremover.

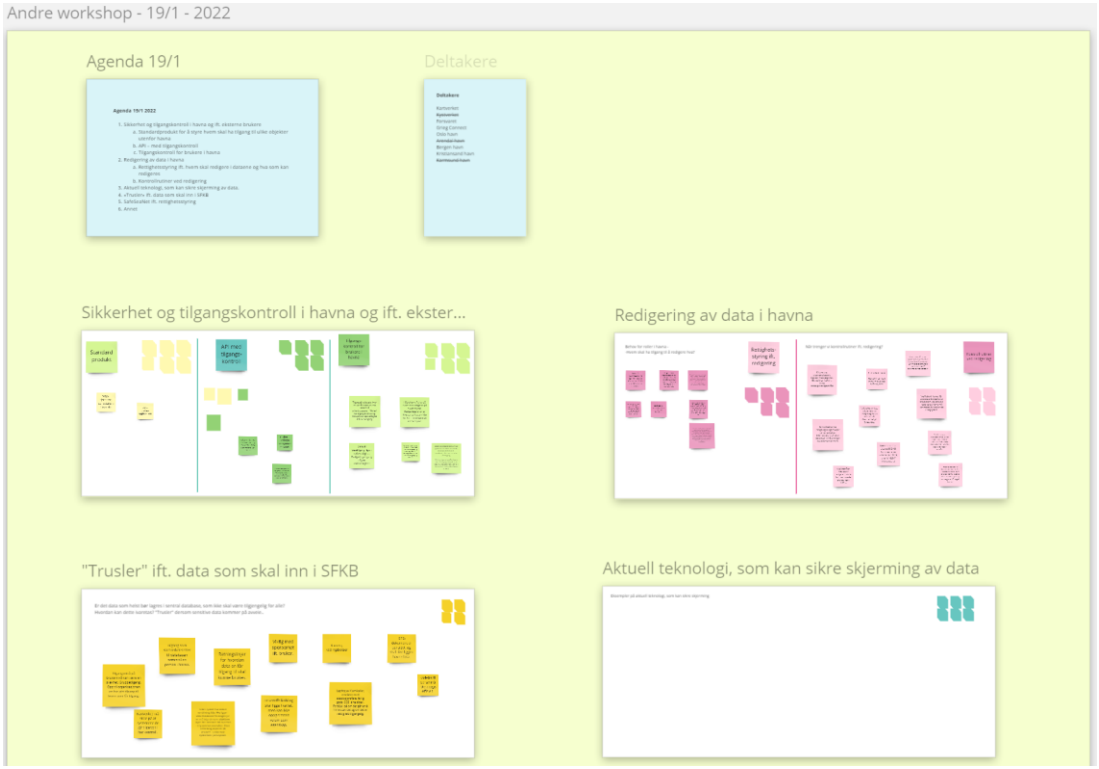
Tidsplan: Arbeidet i arbeidsgruppa vil hovedsakelig foregå i tidsrommet januar – februar 2022. Det skal leveres en rapport fra arbeidsgruppa innen 11.03.2022.

2 KARTLEGGING AV BRUKERBEHOV – RETTIGHETER OG AUTORISASJON

2.1 Metodikk

I arbeidsgruppa er det blitt jobbet med aktuelle temaer i digitale workshops i det digitale white board-verktøyet Miro. Det er blitt avholdt tre workshops i arbeidsgruppa. I tillegg ble det gjennomført et temamøte, der det ble invitert inn aktuelle deltakere utenfor arbeidsgruppa.

- Første workshop, innledende runde. 12.01.2022.
- Andre workshop, 19.01.2022.
- Tredje workshop, 09.02.2022.
- Workshop/Temamøte med tema Akutt beredskap i havn, 16.02.2022.



Figur 1. Utklipp fra Miro-board fra andre workshop, 19/1.2022.

2.2 Temaer som peker seg ut

Følgende temaer har pekt seg ut underveis i arbeidet.

- Hvilke data er sensitive eller har sensitiv informasjon i havnedatastandarden?
- Brukertilgang for havnebrukere
    - Hvem skal ha tilgang til hva?
    - Brukertilgang – lesetilgang – for f.eks. operasjonell drift i havna
- Redigering av data i havna
    - Behov for roller i havna?

    - Hvem skal ha tilgang til å redigere i dataene?
    - Når trenger vi kontrollrutiner ift. redigering?
    - Hva må måles inn før redigering? Hva kan redigeres uten ny innmåling?
- Sikkerhet og tilgangskontroll i havna.
    - Standard produkt med ulike nivåer
    - API med tilgangskontroll
    - Tilgangskontroll for brukere i havna
    - Tilgangskontroll for eksterne brukere
- Trusler ift. data som skal inn i SFKB
- Aktuell teknologi, som kan sikre skjerming av data
- SafeSeaNet ift. rettighetsstyring
- Er det noen av objekttypene i havnedata som er omtalt i sikkerhetsloven?
- Akutt beredskap i havn.

3 BRUKERBEHOV ETTER TEMA

3.1 Hvilke data er sensitive eller har sensitiv informasjon i havnedatastandarden?

Siste versjon av havnedatastandarden, Havnedata 2.0, har 35 objekttyper. Er det noen av disse objekttypene som er sensitive, eller som har egenskaper som er sensitive? Hvorfor er de sensitive? Hvilke hensyn må tas?

HavnId

- Forvaltningsområde
- ForvaltningsområdeGrense
- Havneområde
- HavneområdeGrense
- Havnesensor
- Kamera

HavneanleggId

- Havneanlegg
- HavneanleggGrense
- Havnegjerde
- HavnegjerdeInngang
- Tørrdokk
- TørrdokkGrense
- Flytedokk
- FlytedokkGrense

KaiId

- Kaiområde
- KaiområdeGrense
- Lastbegrensningsområde
- LastbegrensningsområdeGrense
- Slipp
- SlippGrense

ObjektId

- Kaifront
- Fortøyningsinnretning
- Fender
- Kran
- Elkobling
- VAuttak
- Tømmestasjon
- Beredskapspunkt
- Drivstofftilkobling
- Avfallspunkt
- Toalett

Reguleringer

- Fartsrestriksjoner
- FartstrestriksjonerGrense
- Forbudsområde
- ForbudsområdeGrense

Eksempler på sensitive data er sensorer som må skjermes eller havneobjekter som enten kan overvåkes eller som utgjør en annen risiko ift. samfunnssikkerhet. De aller fleste av havnedataene oppfattes likevel ikke som sensitive data av havnene, men det kan være noen egenskaper på enkelte datasett som er sensitive. Selv om ikke alle dataene er sensitive er det ikke nødvendigvis slik at alle brukere av havnedata trenger tilgang til all informasjonen. Det kan fort bli i det meste laget for brukeren å få opp all tilgjengelig informasjon.

Eksempler på informasjon i havna som kan være sensitiv:

- ISPS-dokument er sensitiv informasjon, og skal ikke ligge i havnedata.
- Drivstofftilkobling (kapasiteter). Selve objektet skal ligge i kartet, men det kan ikke oppgis totalt volum som egenskap for allmennheten.
- Elkobling (kapasiteter)
- Havnesensorer (enkelte egenskaper er sensitive)
    - Portsensor, fartsmåler, dørsensor, redningsbøyeskap-sensor
- Kodelås til porter må ikke oppgis offisielt
- Kamera (havnene ønsker ikke at allmennheten får tilgang til plassering av kameraer)
- Områder med eksplosjonsfare
- Beredskapspunkter (enkelte egenskaper)
- Noen av disse punktene bør være tilgjengelig for nødetatene, men ikke for publikum: Angrepsvei, brannalarmsentral, brannfarlige opplag, eksplosjonsfare, nøkkelskap, gass under trykk, Høyspenning (bortsett fra tilkobling til fartøy), røykluke, sprinkleranlegg
- DSB: Godkjente sprengstofflagre (egne registre/kartlag)
- Lagring av farlig last/gods eller kjemikalier (det ligger informasjon om dette på DSB sine sider)
- Sikringstiltak for ISPS havneanlegg (kamera mm.)

3.2 Trusler ift. data som skal lagres i Sentral Felles Kartdatabase (SFKB)

Sentral felles kartdatabase er et forvaltningssystem, der kartdata fra kommunene blir direkte oppdatert i en sentral database hos Kartverket. Kartdatabasen gir alle brukere tilgang til ferske og kvalitetssikrede data (Kartverket, 2021). Data i standarden havnedata 2.0 lagres i SKFB og synkroniseres til og fra havnesystemet fra originalbasen.

Har vi data i havnene, som bør lagres i den sentrale databasen, men som likevel ikke skal være tilgjengelig for alle? Hvordan kan dette ivaretas? Har vi data som rett og slett ikke bør lagres der? Hva er «truslene» dersom sensitive data kommer på avveie? På tidspunktet temaet ble diskutert i arbeidsgruppa, var det ingen som egentlig mente at havnedata på avveie kunne utgjøre en stor trussel. Men mulig truslene vil oppleves som større nå som hele verdenssituasjonen er endret med Russland sin invasjon av Ukraina. Det vil uansett være viktig å ikke publisere sensitive data ut offentlig.

3.2.1 Er det noen havnedata som er omtalt i sikkerhetsloven?

Hva ligger i sikkerhetsloven? Fins det retningslinjer en må følge dersom objektene ligger der. Dette ble tatt opp som tema i en av workshopene, men det var ingen internt i arbeidsgruppa som kunne svare det ut. Det var enighet om at det uansett om havnedata er omtalt i sikkerhetsloven eller ikke bør etableres noen retningslinjer for hvordan data en får tilgang til skal kunne brukes. En bør og få satt i system hva som er sensitiv informasjon, og hva som ikke er det. Dette må ikke være noe som en er usikker på.

3.2.2 Tilgangskontroll mot SFKB

Kartverket må stole på at systemene de gir tilgang til har kontroll. Her er det viktig med sporbarhet ift. bruker. Kartverket har system for rettigheter. Tilgang som Kartverket setter til databasen settes pr. i dag til én person i havna. Det skilles pr. i dag ikke på enkeltbruker nedover i systemet, men f.eks. en bruker pr. havn. Grieg Connect har også tilgang, og videre distribuering av denne tilgangen settes av Grieg Connect i sitt system. Det er opp til organisasjonen en har gitt tilgang til hvem som får tilgang videre. Tilgangskontroll på brukernivå kan potensielt være en svakhet.

3.3 Sikkerhet og tilgangskontroll for brukere i havna

- Tilgangskontroll for brukere i havna – interne og eksterne brukere
    - Er det behov for roller i havna – hvilke roller?
    - Hvem skal ha tilgang til hva?
    - Brukertilgang – lesetilgang – f.eks. operasjonell drift i havna
- Standard produkt med ulike nivåer
- API med tilgangskontroll

3.3.1 Brukertilgang til havnedata for havnebrukere

Tilgangskontroll for interne brukere i havna

Internt i havna baseres tilgang til havnedataene på roller. Hver bruker får tildelt en rolle basert på hvilke arbeidsoppgaver brukeren har. "Rollen" har tilgang til ulike ting. For å få skrivetilgang må det først gis opplæring. Det er litt ulik praksis i havnene på hvordan dette løses praktisk. I mindre havner er det ikke så mange havnebrukere, og er nok ikke nødvendig å skille på brukere med lese- eller redigeringstilgang i samme grad som i en stor havn. I Oslo havn har de en policy på hvem som redigerer på hvilke objekt. De har ansvar for ulike kategorier av havneobjekt. Redigeringsrollen er ikke styrt slik at en ikke har lov til å redigere på andre objekt enn de en har ansvar for, men en skal likevel ikke gjøre det.

I Grieg Connect sitt havnesystem brukes "Public" - for de havnedataene, som skal være tilgjengelig for alle og "private" for objekter som ikke skal være tilgjengelig for alle. Som standard får havnebrukerne

«Lesetilgang» som rolle/rettighet. Etter opplæring kan brukere som havna bestemmer få tilgang til redigering. Dette er en egen rolle/rettighet.

Alt av havnedata som hører hjemme i standarden skal ligge i databasen og synkroniseres til SFKB. Tilgang til dataene kan gjøres med tilgangskontroll. Havna har også mulighet til å flagge objekt som «private» i havnesystemet. Disse objektene synkroniseres ikke inn til SFKB. Det gjelder data som ikke er en del av standarden eller som er under planlegging.

Standardprodukt for WMS-er

Er det behov for mer enn én standard- WMS for havnedata? Slik det er i dag er det satt opp én WMS-tjeneste for visning av havnedata. Denne er f.eks. tatt i bruk i Kystinfo. Det har kommet enkelte tilbakemeldinger på at det for noen blir litt overveldende dersom det er for mye informasjon i tjenesten. Det bør lages en mulighet for å differensiere/skru av og på for brukeren i kartløsningen, for å lette brukeropplevelsen.

Det er viktig å fokusere på produktet som brukerne skal ha – sluttbrukerproduktet. Dette må henge sammen og fungere godt. Kartløsningen må være lagvis ift. brukere og brukerfunksjon. Havnebrukerne, som skal bruke havnesystemet vil være både folk som jobber i havna og folk som kommer fra sjøen. En må velge hva som skal vises for brukerne, slik at en unngår overveldende mye informasjon.

Det foreslås at det som eksterne brukere ser av havnedata, styres med «standardprodukt» for hva som skal ligge i WMS-en. Her bør det ikke opprettes mange WMS-er, da det vil være krevende å drifte, men kanskje en WMS for havnebrukere på land i havna og en for de som ankommer havna for sjøen. Brukere, som trenger tilgang til data utover det som blir tilgjengelig for publikum via Havnedata-WMS, kan få tilgang til data via API med tilgangskontroll.

3.3.2 API med tilgangskontroll

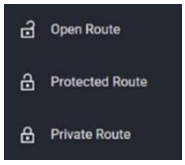
Datatyper og havneobjekter, som er i standarden, skal synkroniseres til SFKB. Det kan styres via et API hvem som får tilgang til objekt som ligger i SFKB. Kartverket har system for å styre hvilke brukere som skal får tilgang. Dette kan brukes for brukere som trenger som trenger tilgang utover det som det gis tilgang til i standard-WMS for Havnedata. Det passer for brukere, som har behov for å kunne styre selv hvilke data de skal få opp.

Forsvaret er eksempel på en bruker, som trenger tilgang til informasjon fra havnedataene utover det som gis i WMS for havnedata. De trenger ikke tilgang til redigering, men de ønsker tilgang til innsyn i dataene f.eks. via API. Sivilforsvaret, Heimevernet osv. trenger tilsvarende tilgang. Tilsvarende kan nødetater ha behov for tilgang til havnedata utover standard WMS-en i en beredskapssituasjon. Dette blir beskrevet lenger nede i dokumentet i kapittel Akutt beredskap i havn. Her ble det foreslått at en setter opp en felles API for beredskapsetater og Forsvaret og gir dem samme type tilgang. Det de ikke trenger kan siles ut.

3.3.3 Rettigheter og roller i Grieg Connect sitt havnesystem

Rettigheter og roller skal føres via en in-house autoriseringsløsning hos Grieg Connect, som heter Tenants. Alle får en standardrolle med leserettigheter som en start. Per i dag er det lagt til rette for rollene «Assets read» (lesetilgang til havneobjekter) og «Assets write» (skrivetilgang til havneobjekter). Superbrukeren har skrivetilgang, og får mulighet til å redigere havneobjekter. Før en havnebruker blir gitt tilgang som superbruker er det viktig at brukeren har fått opplæring.

Foreløpig er det ikke mer oppdelt enn dette. Ved behov vil en gå videre med å legge til rette for mer oppdelt og mer spesifikk rollestyring. Eks. kan det være noen som ønsker å kunne jobbe med anløp etc. men som ikke jobber med kunder.



- Open Route: Tilgjengelig for alle
- Protected Route: Tilgjengelig for en gruppe brukere
- Private Route: Tilgjengelig for enkeltbruker.

3.4 Rettighetsstyring ift. redigering av data i havna

Det er svært viktig at vi ikke mister kvaliteten på havnedataene pga. manglende oppdateringer. Kvalitetssikringskrav er svært relevant med tanke på hvem som skal få lov til å redigere på oppmålte havnedata. Det var enighet i arbeidsgruppa om at krav ift. kvalitetssikring bør komme fra Kartverket. Det bør stilles krav både ift. hva havna kan redigere og hvem som skal få tilgang til det. Men det er også viktig å unngå at kravene som stilles blir så strenge at havnene ikke tør å gjøre viktige oppdateringer.

Når en ser nærmere på hvordan håndtering av redigering av havnedata bør foregår dukker det opp mange spørsmål.

- Er det behov for rettighetsstyrt redigering av havneobjektene i havna? Hvem skal ha tilgang til å redigere i dataene, hva skal de få lov til å redigere og hvordan kan tilgangen styres?
- Skal geografisk plassering/geometri på havneobjekt kunne redigeres uten ny innmåling, og hvilke retningslinjer skal ev. gjelde?
- Er der situasjoner eller kvalitetskrav på noen av objekttypene i havnedatastandarden, som tilsier at en bør praktisere sidemannskontroll ved redigering på egenskaper?

Dagens praksis i havnene for oppdatering/redigering

Bergen havn: I Bergen havn har de en utskiftingsplan ift. pullerter. Dette er en plan for innmåling av nye pullerter, slik at de kan legges inn fortløpende. Det er viktig at kvalitetskrav som stilles til redigering ikke hindrer oppdateringer.

Oslo havn: I Oslo havn skal ca. fem personer inn og redigere på havneobjekter. Personene som skal inn og redigere har ansvar for ulike objekttyper – sortert pr. kategori. Oslo havn tenker seg at det kunne vært greit å kunne sette rettigheter til redigering basert på objektkategoriene. Det er ikke mulig pr. i dag.

Kristiansand havn: I Kristiansand havn har de et vedlikeholds-program for kaifronter. Her brukes Norkyst. Havna ønsker en avtale for å gjøre innmålingen jevnlig.

3.4.1 Kontrollrutiner ved redigering

Det bør etableres kontrollrutiner for redigering av egenskaper og geometri på havneobjekter. Arbeidsgruppa foreslår å klassifisere havneobjektene i to nivå basert på hvor kritiske objektene er ift. innmåling: Nivå 1 og nivå 2. Dette bør beskrives i neste versjon av registreringsinstruksen.

Nivå 1 – Kritiske havneobjekter: Objekter med egenskap for sjøkartnull er kritiske objekter. I Havnedata 2.0 er dette Kaifront og Fortøyningsinnretning, med nøyaktighetskrav på 10 cm og Fender med nøyaktighetskrav på 20 cm. Med tanke på roboter i havna, med sensorerer som sjekker f.eks. tilkoblingsstatus underveis, vil det sannsynligvis kunne være behov for å stille større nøyaktighetskrav til også flere havneobjekter i fremtiden. Lastbegrensningsområde har ikke dette i dag, men ble løftet frem i som et objekt som burde ha det pga. at dette på sikt vil være svært relevant for f.eks. autonome kraner.

Nivå 2 – Andre havneobjekter: Havneobjekter som er ikke like kritiske ift. nøyaktighet. Disse har ikke like strenge krav til nøyaktighet som fortøyningsinnretning og kaifront.

3.4.2 Redigering av geografisk plassering/geometri med eller uten innmåling

Det er viktig å unngå at oppdatering av havnedataene blir så komplisert at havnene kvier seg for å gjøre det. Basert på diskusjoner i workshops i arbeidsgruppa er det foreslått noen retningslinjer. Det ble også løftet frem at det må beskrives i registreringsinstruksen hva Kartverket forventer ift. kvalitetskrav, der det tydelig fremkommer hva som må måles inn og redigeres umiddelbart ved endring på et havneobjekt.

Det er viktig at havnene sikrer at firmaene som går inn og måler inn havneobjektene bruker registrerings-instruksen og tilrettelegger dataene iht. denne. Det bør informeres om at det skal måles iht. registreringsinstruksen allerede i utlysningen. Da sikrer en at kvaliteten opprettholdes ved innmåling. Det kan også være fornuftig for havnene å inngå rammeavtale med firma som måler inn fortløpende eller tar dette jevnlig i et oppsamlings-hit. Et av de tre firmaene som Kartverket har inngått rammeavtale med kan være et fornuftig valg, da disse firmaene allerede er vurdert som godt kvalifisert for oppgaven.

Kvalitetskrav ift. redigering for nivå 1 og nivå 2

Det ble foreslått å bruke nivå 1 og nivå 2 som utgangspunkt for å beskrive hva havna skal få lov til å redigere ift. geometri/geografisk plassering uten ny innmåling.

Nivå 1: I med at nivå 1 – objekter er kritiske ift. navigasjon, bør det stilles krav til at nivå 1 – objekter måles inn med en gang endring på geometri eller geografisk plassering er gjort. Dette gjelder kritiske objekter som har egenskapen sjøkartnull. Det bør lages en liste over kritiske objekt med krav om umiddelbar justering. Foreløpig gjelder dette Fortøyningsinnretning, Kaifront og Fender.

Nivå 2: For øvrige objekter ble det foreslått to mulige løsninger.

- **Alternativ 1**: Det tas en oppsamling av objekter som skal justeres eller legges inn. Havna lager en liste over nye og endrede objekter. Havna legger dem inn/ justerer dem i forbindelse med innmåling. Lista bør beskrive hvilke objekt som har endringer og beskrivelse av endringen. For at dette skal fungere godt må havna ha en god rutine, slik at en sørger for at de blir oppdatert på jevnlig basis. Det må ikke gå for lang tid til de blir oppdatert. Da mister brukere av havnesystemet fort tilliten til at det er oppdatert nok.
- **Alternativ 2**: Havneobjektene justeres av havna fortløpende i havnesystemet, men kvalitetsstempelet på endrede objekt justeres ned dersom de ikke måles inn i forbindelse med justeringen. Kvalitetsstempelet justeres tilbake når havneobjektene er innmålt. De endrede objektene legges inn en liste, som oppmålingsfirma får tilsendt før de skal gå over og sjekke de nye/justerte objektene. Her kan det f.eks. settes et fast innmålingsintervall. Mulig det er behov for en ny egenskap på objektene for å tydeliggjøre om objekt er justert uten innmåling?

3.4.3 Redigering av egenskaper på havnedata

Det anses ikke som nødvendig å stilles like strenge krav med hensyn til redigering av egenskaper på objektene. Men også her kan det være enkelte egenskaper, som er mer kritiske. Eksempelvis er belastning på en fortøyningsinnretning en kritisk verdi. Det kan få store konsekvenser dersom belastningen justeres oppover med en feil. Hvor tung last en kran kan løfte eller hvor stor vektbegrensningen er på et lastbegrensningsområde er også verdier som bør kvalitetssikres før endring. Hvilke krav som skal gjelde bør komme fra Kartverket. Det må komme tydelig frem om det er egenskaper på objektene som er mer kritiske enn andre.

Krav til sidemannskontroll?

En mulig tilnærming kan være å ta i bruk sidemannskontroll for kritiske egenskaper, for å sikre at det ikke legges inn feil verdier på disse. Det bør stilles krav til sidemannskontroll på alt med nivå1 ift. redigering av egenskaper. Nivå 2 trenger ikke sidemannskontroll bortsett fra på evt. enkelte kritiske egenskaper. Det er viktig at disse beskrives tydelig, slik at det ikke glipper. Sporbarhet ift. redigering er også noe som er viktig uansett om havnedataene er på nivå 1 eller nivå 2.

Andre aktuelle tema ift. redigering/oppdatering av havnedata eller data til andre systemer

- Validering av data på vei inn i API-et etter redigering. Det er viktig at geometrifeil gir feilmelding. Data med geometrifeil skal ikke kunne sjekkes tilbake til SFKB.
- Hjelpedatasett fra kommunen kan tas inn i kartløsningene, som brukes i havna. Dette gjøres i Kristiansand og vil og kunne gjøres i Grieg sin løsning. Det fins egne systemer for å ivareta dette i kommunen. Det er lurt å ha et godt samarbeid med kommunen ift. systemer de vedlikeholder. Et

eksempel her er infrastruktur ift. strøm og vann- og avløp. Kommunen har tilgang til QMS-løsningene via GISLINE (Norkart) eller Winmap (Norconsult).

- Vedlikehold i havna: Når arbeidet er ferdigstilt skal firmaet som vedlikeholder rapportere til havna og til kommunen for vedlikehold i riktig system.

3.5 Safe Sea Net ift. rettighetsstyring

Hovedfokuset i Safe Sea Net er på ISPS havneanlegg. I Safe Sea Net er det stor forskjell på om informasjon innenfor et havneanlegg er i et ISPS-anlegg eller i et ikke ISPS havneanlegg. På kai varierer kvaliteten mer i Safe Sea Net enn i Havnedataene.

Havnene må ha gode rutiner for oppdatering i Safe Sea Net. Det er den enkelte havna som har ansvar for å vedlikeholde sine havneobjekt. De skal ikke vedlikeholde informasjon som er i sjøen. Havnene har rutiner for varsling og oppdateringsrunde. Det er kjempeviktig at alle havnene har ambisjon om å holde dataene ved like, slik at vi opprettholder kvaliteten. For å sikre det vil det være viktig med en tydelig visning av om det er noen av havnedataene, som ikke er oppdatert i systemet. Pr. i dag ligger det inne en oppdateringsdato på objektene.

Hvem har tilgang til å redigere/oppdatere inn her?

Havnedataene er en del av grunnlagsdataene i Safe Sea Net, og det er pr. i dag ganske mange som kan gå inn og redigere i grunnlagsdataene der. For å sikre kvalitet i grunnlagsdataene må det være noen superbrukere i havna, som er kvalitetsansvarlig for dataoppdateringen. De som har ansvar for å registrere dataene, må ha litt domenekunnskap. Dataene skal kunne brukes i ulike domener.

Applikasjonen - verktøyet en bruker til å redigere i dataene kan styre hvilken tilgang brukere har til redigering. Brukeren må bekrefte innlogging når den går inn. Det logges både hvilke endringer som er gjort og hvilken bruker som var inne og gjorde endringen. Kystverket har oversikt over alle registreringer/endringer som gjøres i Safe Sea Net. De sier også at det ligger inne ganske mange ansatte, som ikke er aktive. For å ivareta sikkerheten bør det sjekkes med jevne mellomrom om det er noen av disse som bør tas ut av systemet.

Det er viktig å videreføre gode data, slik at en kan stole på det som er der. Det må være et klart krav til at dataene som hentes inn i Safe Sea Net kommer gjennom SFKB/fra Grieg Connect. Det må også være helt tydelig hvem som har ansvar for å oppdatere data, som skal inn i Safe Sea Net. Det kan være fornuftig å sette en eller to som hovedansvarlige for denne redigeringa. Det er også viktig at brukeren som gjør endringer på objekt i Grieg Connect sitt system blir sendt videre til Safe Sea Net, og at en passer på at en unngår dobbeltregistreringer.

3.6 Aktuell teknologi, som kan sikre skjerming av data

Ønske om veileder. Det er et ønske fra havnene om å få på plass en veileder, som beskriver hvordan noen gitte objekter eller attributter skal skjermes. Veilederen skal brukes av havna, for å unngå at skjerma data kommer på avveie. I veilederen bør det beskrives f.eks. om og når en skal bruke totrinns-autentisering, hvilke regler som gjelder for datalagring og retningslinjer for skytjenester og hvor data skal lagres. Det fins norske offentlige instrukser på datasikkerhet, som en sannsynligvis vil kunne ta utgangspunkt i.

Totrinns-autentisering kan være et praktisk sikkerhetsnivå.

Sporing. Kan det være aktuelt å spore hvem som har hentet ut data? Bruk av logg. Per i dag i Port fins det en logg, som beskriver endringer som er blitt gjort på objekt. Fra loggen kan en lese ut hva som er endret, hvem som gjorde endringen og når endringen ble gjort. Et eksempel kan være at det i loggen er oppgitt at maksbelastningen på en pullert ble endret fra 30 til 50, når og av hvem den ble endret.

Datalagring – hvilke regler gjelder? Norske data som er sensitive må lagres i Norge. Eksempelvis lagres graderte dybdedata i Norge, og det kreves sikkerhetsklarering for å få tilgang til disse.

Skytjenester -på hvilket land sin grunn skal de legges? Bør en stille krav til at dataene skal lagres på norsk grunn? Dersom norske data og tjenester lagres utenlands er det viktig å være obs på hvilken juss som gjelder i landet dataene lagres. Det er viktig å ha en avtale der en sikrer at Norges krav ivaretas. En må sette krav til dataene.

Rettigheter og rollestyrt tilgang. Kartverket kan gi rettigheter til Grieg Connect - som gir rettigheter videre til sine brukere. En del havner får rettigheter fra Grieg Connect + rettigheter fra Kartverket. Det er viktig å ha kontroll på hvem som har tilgang til hva.

Det kan defineres roller for brukere av basen i havnesystemet. Rollen låser hvilke objekter en gitt rolle skal ha tilgang til. Rollen må låses på objektnivå, og kan ikke styres til egenskaper. Brukeren selv – altså havna – må velge hvilke egenskaper som distribueres ut. Det angis i den interne delen av systemet.

ISPS- områder er gradert etter sikkerhetsloven. Der er det begrenset tilgang og ulike nivåer. Det ble stilt spørsmål til om dataene innenfor områdene skal inn i databasen. Det var enighet i at data som havna skal ha tilgang til bør legges inn i en felles database, selv om ikke alle skal ha tilgang til lat. Med bakgrunn i dette bør det holdes igjen litt ift. tilgang før en legger alt ut åpent. Skjerming av data innenfor ISPS-områder bør være default, slik at havna selv kan gå aktivt inn og avskjerme objekt som ligger der.

Risikoanalyse av systemet kan være et krav. Hvor er sårbarheten i systemet? Her bør en tenke sikkerhet i flere nivå. Jo høyere graderte data en tar inn, jo flere krav kommer. Vi har f.eks. pr i dag ett graderingsregime på dybdedata. All høyoppløselig dybdedata (med unntak av spesifikke frigitte områder) er gradert. Høyoppløselig dybdedata er der hvor det er mindre enn 50 meter mellom punktene. Dersom 0 – 30 m dybde blir frigitt forandres graderingsregime på dybdedata.

Personvern – GDPR må hensyntas ift. skjerming. Persondata skal ikke lagres over tid. Ikke aktive brukere må ut av systemet. Det er viktig at en får etablert rutiner for hvordan en sikrer at dette blir gjort i havna. Kartverket har retningslinjer på eiendomsobjekt. Forslag om at kontaktpersoner, telefonnummer og e-postlister kan lagres i en database, der en sørger for å ha egne regimer som skal gjelde for persondata.

Det fins informasjon om PFSO-er (Port Facility Security Officer) på hvert enkelt havneanlegg. Informasjonen ligger på Safe Sea Net og slettes årlig for å ivareta personvernhensyn.

3.7 Akutt beredskap i havn

Hvilke data trengs det tilgang til ved akutt beredskap i havn? Hvilke opplysninger trenger beredskapsetatene fra havna? Vil tilgang via et API fungere bra?

Havnene bruker litt forskjellige krisehåndteringsløsninger for håndtering av akutt beredskap i havna. Eksempelvis bruker Bergen havn «Reiven» - krisehåndteringsløsning for havner ift. beredskap mens en i Oslo havn bruker Incaseit – kriseberedskapsverktøy.

Beredskapsplan: I hver havn skal det utarbeides en beredskapsplan, som beskriver hvilke handlinger en skal gjøre ved en akutt hendelse i havna. Kommuner eller havner har ansvar for å utarbeide beredskapsplaner.

3.7.1 Brann i havna

Låste porter/sikra anlegg

Brannvesenet har tilgang og kort til alle porter for enkel tilgang ved beredskapssituasjoner. 110-sentralen har tilgang til å komme gjennom låste bommer. Oslo havn melder om at det noen ganger er hengelås/kort på porter, og at de byttes ut av og til. Er det gode nok rutiner for å at brannvesenet får de tilgangene de trenger?

Behov for datatilgang ved beredskapssituasjoner

Det kan se ut til at beredskapsetatene får tak i det meste de trenger fra andre databaser, og vi må unngå at det blir mange kilder det skal hentes data fra. Derfor er det viktig at vi er obs på andre databaser, som går parallelt. Elverk og kommuner sitter på lokale databaser av ymse slag. Flere havner samarbeider allerede godt med kommunen, og får tilgang til data fra dem. Bergen havn får f.eks. data fra kommunen månedlig. Kommunene har flere datasett som synkroniseres til felles base, og har mulighet til å gi tilgang via API. Det er mulig å koble seg opp mot en relativt oppdatert datastrøm derfra. For elverk er det delvis felles standard, men det kan være vanskelig å få tak i dataene raskt, da det ikke er API-tilgang til dem.

Det som vil være viktig ift. beredskap er å lokalisere hvilke data i havnedatabasen det er behov i beredskapssituasjoner, som ikke er tilgjengelig andre steder. Det kan være smart å ha en datamodell, som fanger opp mange muligheter, og tilgang via API er nyttig.

Kommunen skal ha kontroll på brannhydranter og brannkummer i eget anlegg. Dette ligger i VA-basen til kommunen. Ift. beredskap vil det være viktig å finne ut hvor den offentlige tilkoblingen ligger. Noen ganger kan den ligge utenfor havneområdet. Endringer som gjøres i havna ift. vann og avløp skal rapporteres til kommunen. Eks. på dette er endringer som påvirker vannledninger.

Kontaktpersoner i havna

Tidlig varsling og det å ha en kontaktperson å forholde seg til er svært viktig i en beredskapssituasjon. Dersom det går alarm direkte fra anlegget har en stort sett kontaktpersoner å forholde seg til. Det er likevel nyttig og relevant for alarmsentralen å ha en oppdatert oversikt over kontaktpersoner i havna. Det er også viktig at kontaktpersonene i oversikten går på hele havna og ikke pr. bygg, da dette blir for detaljert informasjon. Dersom det er mulighet for å tilgang til kontaktpersonene med et API hadde det vært veldig interessant for 110-sentralen.

Det er også viktig med oppdatert kontaktinformasjon til aktørene som befinner seg i havna. Alle som trenger det, må få rask beskjed ved en krisesituasjon slik som f.eks. brann.

Kritiske objekt

Kritiske objekt kartlegges av brannvesenet ved befaring. Eks. på dette er brannvarslingsanlegg, som er stedet en møter opp først ved alarm. Utstyr i havna skal være godt merka, slik at en vet hvor en finner dem. Dette kontrolleres av brannvesenet ved befaring.

Hjertestartere. Det fins allerede et register for hjertestartere, som beredskapsetatene har tilgang til. De trenger dermed ikke tilgang til dette fra Havnedata. Hjertestarterregisteret - Finn nærmeste hjertestarter | 113.no

Farlig last – Lokus. DSB har oversikt og 110-sentralen har tilgang inn her i fastregisteret pr. dags dato. Ikke behov for at dette lagres flere steder. Det som har innvirkning på mannskapene, bør prioriteres først.

Sikringsradio som backup

Dersom det er behov for beredskap i områder uten mobildekning brukes sikringsradioen. Denne er backup for mobiltelefon. 110-sentralen har f.eks. tilgang til kontaktpersoner på oppdretts-anlegg via denne, noe som er nyttig ved brann f.eks. på oppdrettsanlegg. Via sikringsradioen blir hvert anlegg oppdatert med den som til enhver tid har ansvar på anlegget. Er dette noe som er aktuelt å bruke som backup også for havner – dersom mobilnettet faller ut?

3.7.2 Brukerhistorie – Brann i et fartøy

Brann ved kai

Brann i fartøy som ligger til kai behandles av det lokale brannvesenet som en bygningsbrann.

Prioritet 1 er å etablere kontakt med bro, hente informasjon om skipet og etablere kontakten med kjentmann ombord. Alle skip er bygd opp rundt en brannstruktur. Nr. 2 om bord er normalt brannvernleder, og vil være kjentmann på skipet mot det lokale brannvesenet. Ritsgruppa/prosjektet har ansvar for å håndtere maritime kriser, men har ikke ansvar for skip som ligger til kai.

Risikoanalyse basert på gammel kunnskap. Beredskapsplan skal være på plass før ulykken skjer. En må vite hvor en finner utstyret. Hvilke båter ligger i nærheten og må flyttes?

Bilde 1. RITS-øvelse. Beredskap ved kai (Foto: Stein Roger Bjørheim).

Brann i skip til sjøs

Brann i fartøy til sjøs håndteres ikke av lokalt brannvesen, men av Ritsgruppa. De har ansvar for å håndtere maritime kriser. For å yte bistand til skip ved ulykker til sjøs har staten inngått avtale med syv brannvesen, som har særlig kompetanse og trening for bistand til skip. RITS | Direktoratet for samfunnssikkerhet og beredskap (dsb.no).

Brannsikkerheten på skip reguleres av sjøfartslovgivningen. Brannsikkerheten om bord er avhengig av at en har gjort forebyggende tiltak og at skipet har en beredskap som fungerer. Skipets egen besetning og forebyggende tiltak om bord utgjør fartøyets primære beredskap. Landbasert brannvesen bistår med sekundær innsats dersom det er behov for det.

På DSB sine nettsider står det at *«Brannvesenet har etter anmodning plikt til å bistå ved branner og andre ulykkessituasjoner i sjøområder innenfor eller utenfor den norske territorialgrensen. Plikten er generell og gjelder alle brannvesen med kysttilhørighet. Grunnlaget for bistandsplikt fremgår av lov om brann- og eksplosjonsvern § 11, inndeling av havnedistrikter og en geografisk avgrensning som normalt sammenfaller med kommunenes grenser, havneloven § 14. En særskilt ordning med beredskap til sjøs for å yte innsats ved branner og ulykker utenfor havnedistriktet, danner behovet for en fastsatt regulering.»*

Bilder 2. RITS-øvelse (Foto: Stein Roger Bjørheim).

3.7.3 Brukerhistorie – Et skip har gått på grunn i fjorden, og det lekker ut olje fra skipet.

Hva er behovene til beredskapsetatene? Hva trenger de fra havna? Det er viktig å få rask oversikt over hvor en finner beredskapspunkt i havna, når uhellet er ute. Det er også viktig å få oversikt over nærmeste depot og kapasiteter.

Prioritet 1: Få oversikt over kapasiteter

- Lagring
- Behandling
- Finne en egnet plass til fram skudd av depot
- Få oversikt over sjøgående ressurser
- Utstyrslager – hvor kan det settes opp?
- Datagrunnlag: dybdedata, infrastruktur.

Kystverket har 15 oljeverndepot langs norskekysten. De er utstyrt med oljelenser, oljeopptakere, strandrense- og nødlosseutstyr (Kystverket, 2021). Plasseringen på disse kan en finne på https://kystinfo.no, under temalag for beredskap. I egenskapene til beredskapsdepot finner en lenke til faktaark der det er opplistet hvilket utstyr som er tilgjengelig i depotet.

4 OPPSUMMERING BRUKERBEHOV OG ANBEFALINGER TIL VEIEN VIDERE

	TEMA	OPPSUMMERING	ANBEFALINGER TIL VEIEN VIDERE
1	**Sensitive data eller sensitiv informasjon**	• De aller fleste av havnedataene oppfattes ikke som sensitive data av havnene, men det kan være noen egenskaper på enkelte datasett som er sensitive. • Noen data bør være tilgjengelig for nødetater, selv om det ikke legges åpent tilgjengelig for allmennheten. • Data kan lagres i SFKB, og havna kan selv velge hvilke data som skal gjøres tilgjengelig for publikum fra havneportalen.	• Ønske om en veileder for havnene, som beskriver hva som er sensitiv informasjon og hvordan den kan sikres/skjermes.
2	**Havnedata og sikkerhetsloven**	• Ikke kompetanse på sikkerhetsloven opp mot havnedata i arbeidsgruppa.	
3	**Sikkerhet og tilgangskontroll i havna**	• Tilgangskontroll for interne bruker basert på roller i havnesystemet. • Behov for tilgangsstyrt tilgang til API for eksterne brukere – eks. beredskapsetater og Forsvaret. • Ønske om kvalitetskrav nivå 1 og nivå 2 på havnedata, der nivå 1 er havnedataobjekt som er kritiske ift. sikker navigasjon.	• Ta stilling til om det er behov for videreutvikling av den rollestyrte tilgangen i havna. Bør vurderes å lage roller basert på behov, f.eks. egen rolle for operasjonell drift. • Oppsett av API for havnedata med tilgangskontroll. • Nivå 1 og nivå 2-objekter bør beskrives i neste versjon av registreringsinstruksen
4	**Brukertilgang for havnebrukere**	• Det kan være overveldende mye informasjon å ta inn for ulike brukere i havna. Pr. i dag får alle brukere av WMS-tjenesten samme informasjon.	• Foreslås å utvikle standardprodukt for WMS-tjenestene for havnedata. F.eks. to ulike oppsett der ett er for bruk i selve havna, og det andre for de som ankommer fra sjøen.

5	**Redigering av havnedata**	• Retningslinjer for hva havnene har lov til å redigere av egenskaper/geometri/geografisk plassering uten at det gjøres ny innmåling. • Behov for å etablere kontrollrutiner for oppdatering av enkelte objekttyper og enkelte egenskaper.	• Etablere tydelige retningslinjer fra Kartverket på hva havnene har lov til å redigere uten ny innmåling. To forslag til alternativer for retningslinjer: 1. Lage liste med objekt som skal endres/legges til og oppdatere først etter innmåling. 2. Endring av kvalitetsstempel på endrede objekt inntil ny innmåling. • Forslag til kontrollrutine: Sidemannskontroll på enkelte egenskaper eller endringer på nivå 2 – objekter kan også være aktuelt for å sikre at ikke noe glipper ved redigering. • Lage en oversikt over hvilke objekttyper og hvilke egenskaper som krever kontrollrutiner.
6	**Trusler ift. data, som skal inn i SFKB.**	• Tilgang til databasen settes per i dag av Kartverket i til en person i havna eller til en organisasjon, f.eks. Grieg Connect. Videre distribuering av tilgang kan settes av Grieg Connect i havnesystemet. • Det er viktig å ikke gi offentlig tilgang til sensitive data. • Det er viktig at brukere av data i havna vet hvordan dataene kan brukes og distribueres.	• Det bør vurderes om dagens tilgangsstyring er god nok. • Det bør etableres retningslinjer for hvilke data som ikke kan være offentlig tilgjengelig. • Det bør etableres retningslinjer for hvordan data en får tilgang til kan brukes.
7	**Aktuell teknologi, som kan sikre skjerming av data**	• Data innenfor ISPS-områder kan være sensitive. De vurderes av havna ift. visning i havnesystemet. Behov for retningslinjer for: • Totrinns-autentisering • Sporbarhet ift. hvem som henter og endrer data • Data og skytjenester bør lagres i Norge	• Data innenfor ISPS-områder bør som default settes til ikke aktiv. Havna selv bør inn og vurdere hvilke data som skal vises i disse områdene. • Se videre på aktuell teknologi for skjerming av data og lage retningslinjer for disse.

		• Rollestyrt tilgang til havnedata • Personvern/GDPR • Risikoanalyse av systemet	
8	**SafeSeaNet ift. rettighetsstyring**	• Behov for rutiner for oppdatering i Safe Sea Net for havnene. • Rollestyrt tilgang, men mange brukere – ikke aktive brukere må tas ut av systemet. • Behov for kontroll på hvilke objekt som ikke er oppdatert i systemet.	• Hver havn bør ha person(er) med hovedansvar for oppdatering til Safe Sea Net. • Hvilke brukere som har tilgang til Safe Sea Net i havnen må gjennomgås regelmessig av havna. • Etablere rutiner for objektoppdateringer.
9	**Akutt beredskap i havn**	• Kontaktpersoner og beredskapspunkt er viktig. Rollestyrt tilgang til API for havnedata hadde vært bra for beredskapsetatene. Med tilgang til dette vil de kunne hente ut de dataene de har behov for til beredskapssituasjoner. • Behov for å lokalisere hvilke data i havndatabasen det er behov for i beredskapssituasjoner, som ikke er tilgjengelig andre steder.	• Oppsett av API for rollestyrt datatilgang utenfor havna. Aktuelt for beredskapsetater og forsvaret. • Lage en liste over data i havnedatabasen, som beredskapsetatene ikke henter andre steder.

Tabell 1. Oppsummering av brukerbehov og veien videre.