Sted og dato:

Innholdsfortegnelse

1	KS-0995B Cybersikkerhet
1.1	Identifisering
1.2	Beskyttelse
1.3	Rapporter og analyser av avvik og feil
1.4	Respons
1.5	Gjenoppretting

1	**KS-0995B Cybersikkerhet** **Veiledning:** Ved avvik på Cyber i de vanlige revisjonssjekklistene på rederikontor og ombord i alle skip, skal denne sjekklisten brukes: Cyberrisiko skal bli ivaretatt på lik linje som andre risikoer om bord. Avvik og observasjoner skal gis for cybersikkerhet når objektive bevis finnes og kan hjemles i forskrift, ISM-koden og rederiets styringssystem. Verifikasjon av cyberpunktene forutsetter åpne spørsmål, demonstrasjon av praksis og vurdering av forståelse. Unngå ja/nei-spørsmål. Det henvises til elementer fra ISM-koden samt til bransjeveiledning Med veiledning menes "THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS" (BIMCO m.fl.) Definisjoner: CRM - Cyber Risk Management Cyber Security Risk Management (CRM) prosessen med å identifisere, analysere, vurdere og informere om en cyberrisiko og akseptere, unngå, overføre eller redusere den til et akseptabelt nivå. Operasjonsteknologi (OT) - datatekniske metoder og verktøy som overvåker og kontrollerer fysiske enheter om bord som ECDIS, automasjon av fremdriftsmaskineri, osv

Nr.	Tekst	Hjemmel/henvisning	Påleggkode	Alvorsgrad	Status*	Anmerkning
1.1	**Identifisering**					

Nr.	Tekst	Hjemmel/henvisning	Påleggkode	Alvorsgrad	Status*	Anmerkning

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

Sted og dato:

1.1.1	**Identifisering av digitale trusler og trusselaktører** Har dere identifisert digitale trusler? Veiledning Eksempler på trusler: – skadevare som spres via vedlegg og lenker i e-post, Microsoft Office-filer eller via infiserte nettsider – lagringsmedier (USB-pinner) kan bli infisert bare ved at de settes inn i en infisert datamaskin – løsepengevirus – sosial manipulering - GPS spoofing (Manipulering av GPS signaler/ motta falske signaler) – man-in-the-middle (angriperen går inn og kontrollerer kommunikasjonen mellom to parter, risiko ved f.eks. trådløse nettverk) – session hijacking (øktkapring) – ID-tyveri – falske trusler og utpressingskrav – phishing (digital fisking etter sensitiv informasjon, passord eller kredittkortnummer) – hacking av konto – datainnbrudd	ISM 1.2.2 Vurderere alle identifiserte risikoer på skipet, personellet og miljøet mm. BIMCO Veiledning kap 2 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2599			
1.1.2	**Identifisering av sårbarheter** Har dere identifisert sårbarheter? Veiledning Har dere identifisert systemer ombord som er sårbare for digitale sikkerhetshendelser? Eksempler på dette: – programvarebaserte kontroll -og automasjonssystemer – programvarebaserte navigasjons- og kommunikasjonssystemer ombord – softwarebaserte Informasjonssystemer ombord	ISM 1.2.2 Vurderere alle identifiserte risikoer på skipet, personellet og miljøet mm. BIMCO veiledning kap 3 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2599			

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

Sted og dato:

1.1.3	**Risikoanalyse** Har dere vurdert risiko knyttet til digitale trusler og sårbarheter? Er det gjort en analyse av risikoene? Veiledning Følgende spørsmål kan brukes som utgangspunkt ved vurdering av cyberrisiko om bord i skip: – Hvilke verdier står i fare? – Hvilke konsekvenser kan en cyberhendelse ha? – Hvem har det endelige ansvaret for cyberrisikostyring? – Er OT-systemene (operasjonsteknologi) og -miljøet beskyttet mot Internett? – Er fjerntilgang til OT-systemene mulig? Hvis ja, hvordan kan slik tilgang overvåkes og beskyttes? – Er IT-systemene beskyttet, og blir fjerntilgang overvåket og styrt? – Hvilke former for cyberrisikostyring blir brukt? – Hvor mye opplæring har personellet som bruker IT- og OT-systemene? • Er risikoer knyttet til cybersikkerhet identifisert og vurdert? • Tiltak som er iverksatt for å kontrollere risiko skal fastsettes basert på risikovurdering hvor det tas hensyn til informasjonen gitt i retningslinjene “Cyber security onboard ships”. • Har de foretatt en risikovurdering der både teknisk utstyr og styrende dokumenter er vurdert? • Som utgangspunkt, bør følgende tiltak vurderes før en risikovurdering foretas: – maskinvare - utvikle og vedlikeholde et register over all kritisk programvare ombord, inkludert autoriserte og uautoriserte enheter i selskapskontrollerte nettverk. – programvare - utvikle og vedlikeholde et register over all	ISM 1.2.2 Vurderere alle identifiserte risikoer på skipet, personellet og miljøet mm. Bimco veiledning kap 4 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2599			

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

	autorisert og uautorisert programvare som kjøres på firmaets maskinvare ombord, inkludert versjon og oppdateringsstatus. SMS en skal oppdateres til å inkludere prosedyrer for: o opprettholdelse av registeret når maskinvare og programvare kontrollert av selskapet erstattes eller oppdateres o godkjenning av installasjon av ny eller oppgradert programvare. o forhindring av installasjon av uautorisert programvare og sletting av slik programvare dersom identifisert o vedlikehold av programvare					
1.1.4	**Politikk for sikkerhet og miljøvern** Er politikk for sikkerhet og miljøvern oppdatert med hensyn til risikoer knyttet til digitale trusler? Veiledning En oppdatert politikk for sikkerhet og miljøvern bør inneholde: • forpliktelse til å håndtere cyber risiko som en del av sikkerhetsstyringssystemet • forståelse av at det er behov for tekniske barrierer, styrende dokumenter og kontrolltiltak for å hindre negativ påvirkning eller avbrudd i OT med hensyn til sikker drift av skipet og miljøvern	ISM 2 BIMCO Veiledning kap 1.1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2510			

Sted og dato:

1.1.5	**Selskapets ansvar og myndighet** Er ansvar og myndighet for cyber risikostyring definert og inkludert i selskapets organisasjonsoversikt? Veiledning Definering av ansvar og myndighet må inkluderes og oppdateres for CRM. Dette inkluderer: • plassering av ansvar og myndighet som oppmuntrer til samarbeid mellom IT personell og selskapets drifts-personell og teknisk personell (kan være tredjepart) • ansvar og myndighetsforhold for skipsfører IT personell skal forstå sårbarheter i databaserte systemer og kjenne til egnede tekniske og styrende dokumenter for å sikre tilgjengelighet og integritet i systemer og data. Drift-spersonell og teknisk personell skal generelt forstå hvordan forstyrrelser i kritiske systemer om bord påvirker sikkerhet og miljøvern.	ISM 3 BIMCO veiledning kap 1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2515			

Sted og dato:

1.1.6	**Ressurser og personell** Er det tatt hensyn til CRM i selskapets prosedyrer for å identifisere opplæring som kan være nødvendig som støtte for sikkerhetsstyringssystemet, og er slik opplæring innført? Veiledning Cyber-bevissthetsopplæring er ikke et obligatorisk krav, men er viktig for grunnleggende forståelse av CRM og hvilken betydning den enkeltes handlinger har for den digitale sikkerheten om bord. Selskapet skal identifisere opplæringsbehov og ha prosedyrer som sikrer at: • alt personell i selskapet får grunnleggende cyber-bevissthetsopplæring for støtte til selskapets CRM, politikk og prosedyrer • personell som har blitt tillagt CRM-plikter får relevant digital sikkerhetsopplæring som samsvarer med deres ansvar og myndighet	ISM 6.5 BIMCO veiledning Kap 5.2 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2530			
1.1.7	**Vedlikehold av skip og utstyr** Er OT og IT inkludert i eksisterende prosedyrer for å identifisere utstyr og tekniske systemer som kan forårsake farlige situasjoner ved en plutselig svikt? I utgangspunktet skal det i et eksisterende sikkerhetsstyringssystem være identifisert utstyr og tekniske systemer (inkludert OT og IT) som kan forårsake farlige situasjoner dersom de blir utilgjengelige og upålitelige. Når CRM skal innføres i et eksisterende sikkerhetsstyringssystem, må man ta hensyn til risikoen for tap av digitale data ved en plutselig svikt. Tap av tilgjengelighet eller integritet til data brukt av kritiske systemer kan ha samme innvirkning på sikkerhet og miljø som om systemet blir utilgjengelig eller upålitelig av andre årsaker.	ISM 10.3 BIMCOveiledning 3 og 4 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2550			

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

Sted og dato:

1.2	**Beskyttelse**					
Nr.	**Tekst**	**Hjemmel/henvisning**	**Påleggkode**	**Alvorsgrad**	**Status***	**Anmerkning**
1.2.1	**Tiltak** 1. Er fysiske tiltak iverksatt? 2. Har de oppdatert prosedyrer, planer og instruksjoner for identifiserte cyber risikoer og risikoreduserende tiltak ? Veiledning: Ta stikkprøve kontroll av identifiserte cyber risikoer. – nettverksbeskyttelse og effektiv av deling – deteksjon av innbrudd/angrep – regelmessig sårbarhetsskanning og -testing – godkjenning av programvare – tilgangs- og brukerkontroll – gode prosedyrer for bruk av passordregler og flyttbare lagringsenheter – personellets kjennskap til risiko og kunnskap om egnede prosedyrer	ISM Kode 7 BIMVO veiledning kap 6 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2535			

Sted og dato:

1.2.2	**Beredskap** Er cybersikkerhet inkludert beredskapsplanene om relevant? Her er en ikke-uttømmende liste over cyberhendelser som bør tas med i beredskapsplaner om bord: – tap av tilgjengelighet til elektronisk navigasjonsutstyr eller tap av integriteten til navigasjonsrelaterte data – tap av tilgjengelighet eller integriteten til eksterne datakilder, som GNSS – tap av viktig forbindelse til land, som tilgjengelighet til GMDSS-kommunikasjon (verdensomspennende nød- og sikkerhetssystem til sjøs) – tap av tilgjengelighet til industristyringssystemer inkludert framdriftssystemer, hjelpesystemer og andre kritiske systemer samt tap av integriteten til datastyring og – kontroll ved ransomware eller overbelastningsangrep Beredskapsplaner og lignende bør være tilgjengelig i ikke-elektronisk form, ettersom noen typer cyberhendelser kan føre til sletting av data og stenging av kommunikasjonskanaler.	ISM kode 8.1 BIMCO veiledning kap 6 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2540			
1.3	**Rapporter og analyser av avvik og feil**					
Nr.	**Tekst**	**Hjemmel/henvisning**	**Påleggkode**	**Alvorsgrad**	**Status***	**Anmerkning**

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

Sted og dato:

1.3.1	**Rapporter og analyser av avvik, ulykker og farlige hendelser** Har selskapet oppdatert avvikssystemet slik at det inkluderer behandling og korrigerende tiltak ved cyberhendelser? Veiledning En eksisterende SMS bør allerede adressere prosedyrer knyttet til avvik. Selskapets rapporteringskrav for avvik må oppdateres for å inkludere cyberhendelser. Eksempler på slike avvik og cyberhendelser: - uautorisert tilgang til nettverksinfrastruktur - uautorisert eller utilpassede bruk av administratorrettigheter - mistenkelig nettverksaktivitet - uautorisert tilgang til kritiske systemer - uautorisert bruk av flyttbare medier - Uautorisert tilkobling av personlige enheter - sviktende etterlevelse av vedlikeholdsrutiner/-prosedyrer for programvare - manglende oppdatering av virusprogram – tap eller forstyrrelse av tilgjengelighet til kritiske systemer – tap eller forstyrrelse av tilgjengelighet til data som kreves av kritiske systemer	ISM kode 9.1 BIMCO veiledning kap 5.1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2545			
1.4	**Respons**					
Nr.	**Tekst**	**Hjemmel/henvisning**	**Påleggkode**	**Alvorsgrad**	**Status***	**Anmerkning**

Sted og dato:

1.4.1	**Ansvarsforhold ved tap av kritiske systemer** Hvordan sikrer selskapet at tilstrekkelige ressurser og landbasert støtte er tilgjengelig for å kunne respondere på tapet av kritiske systemer? Veiledning En godkjent SMS skal beskrive ansvar, myndighet og forhold mellom alt personell som leder, utfører og verifiserer arbeid knyttet til CRM. Integrering av CRM krever nødvendig IT-kompetanse og ressurser. Dette kan være inkludert i selskapet eller levert fra tredjepart. Følgende bør vurderes: - selskapets- eller en tredjeparts tekniske support skal være kjent med IT- og OT-infrastruktur og systemer om bord - ethvert internt responsteam eller eksternt cyber-beredskapsteam skal være tilgjengelig for å gi støtte til ansvarlig person ved behov.	ISM kode 3.3 BIMCO veiledning kap 7.1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2515			

Sted og dato:

1.4.2	**Vedlikehold av skip og utstyr** Har selskapet oppdatert de spesifikke tiltak som er rettet mot å fremme påliteligheten til OT? En godkjent SMS bør inneholde prosedyrer for driftsvedlikeholdsrutiner for å fremme påliteligheten til utstyr og tekniske systemer som kan forårsake farlige situasjoner ved plutselig svikt. SMS bør inneholde dokumentert fremgangsmåte for: – vedlikehold av programvare som en del av driftsvedlikeholdsrutinene. Slike prosedyrer skal sikre at programvareoppdateringer blir utført og testet av en kompetent person. – autorisasjon for ekstern tilgang til kritiske systemer for programvare- eller andre vedlikeholdsoppgaver. Dette bør omfatte autorisasjon av tilgang generelt. , inkludert bekreftelse av at tjenesteleverandører har truffet egnede beskyttelsestiltak selv. – hindring av programvareoppdateringer ved ukontrollerte eller infiserte flyttbare medier (f.eks. minnepinne) – kontroll av administratorrettigheter for å begrense vedlikeholdsoppgaver for programvare til kompetent personell	ISM kode 10.3 BIMCO veiledning kap 7.1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2550			
1.5	**Gjenoppretting**					
Nr.	**Tekst**	**Hjemmel/henvisning**	**Påleggkode**	**Alvorsgrad**	**Status***	**Anmerkning**

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon

Sted og dato:

1.5.1	**Vedlikehold av skip og utstyr** Er rutiner for vedlikehold- og testing av backup ordninger for utstyr om bord inkludert i skipets vedlikeholdsrutiner? Veiledning: Sikkerhetsstyringssystem bør inneholde prosedyrer for vedlikehold og testing av backup ordninger for utstyr om bord. SMS bør inneholde prosedyrer for: – kontroll av backup backupordninger for kritiske systemer – vedlikehold og lagring av offline datasystemer (backup av data og systemer). – kontroll av alternativ driftsmodus for kritiske systemer (dersom dette ikke allerede er dekket i eksisterende prosedyrer) – vedlikehold av backup av data som er nødvendige for sikker drift av kritiske systemer – periodisk testing av backup og backup rutiner.	ISM kode 10.4 BIMCO veiledning kap 1 og 7.1 / FOR 2014-09-05 nr. 1191 Forskrift om sikkerhetsstyringssystem for skip m.m. .	2550			

* **A**: Akseptert **IR**: Ikke relevant **P**: Pålegg **K**: Kommentar **F**: Funn fra revisjon