

QUESTIONNAIRE

Cyber Cover

To qualify for cyber coverage, we require you to complete a questionnaire in collaboration with us. This document provides a comprehensive list of all the necessary questions to ensure you are fully prepared.

1. Company details

Question	Type	Description
1.1 Authority Name	Text input	Name of person completing the application
1.2 Authority Position	Text input	Position of person completing application
1.3 Policy holder legal address	Text input	The legal address of the organization
1.4 Organisation(s) and sub-organisation(s)	Text input	
1.4.1 Organisation numbers(s)	Text input	
1.4.2 Organisation names(s)	Text input	
1.4.3 Organisation country/countries of operation	List	
1.5 Most recent fiscal year total annual enterprise revenue (USD)	Value	

2. Vessels

Question	Type	Description
2.1 Vessel(s)	List	List all vessels
2.1.1. Vessel name / IMO number	List	List retrieved from database
2.1.2. Day rate(s) (USD)	List	List all vessel day rates
2.1.3. Vessel value (USD) (Retrieved from database)	List	List retrieved from database

3. IP addresses and domains

Question	Type	Description
3.1 IP Addresses	List	List all IP addresses
3.2 Domains	List	List all domains

4. Cyber security frameworks and certifications

Question	Type	Description
4.1 Does your company have ISO27001?	Yes/No	
4.2 Which ISO version?	Text input	Only applicable if you have ISO27001
4.3 Do you have an digital copy of certification document(s)?	Yes/No	
4.4 Upload digital copy of certification document(s)	File upload	Only applicable if you have a digital copy of certification document(s)
4.5 Which Cyber Security Framework/s does the company adhere or align to?	Text input	For example NIST.
4.6 Do you have an digital copy of the framework and control measures?	Yes/No	
4.7 Upload digital copy of the framework and control measures document(s).	File upload	Only applicable if you have a digital copy of the framework and control measures

5. Subsidiaries

Question	Type	Description
5.1 Organisation(s)	List	List all organizations/subsidiaries
5.2 Do you have a documented cyber security policy?	Yes/No	Per organization
5.3 Do you have an digital copy of your policy document?	Yes/No	Per organization. Only applicable if you have documented cyber security policy
5.4 Upload policy document(s)	File upload	Per organization. Only applicable if you have a digital copy of your policy document(s).
5.5 How often do you review the cyber security policy?	Selection	Per organization. Annually, less or never.
5.6 Do you have an asset register?	Yes/No	Per organization.
5.7 Does the asset register include a list of all hardware devices that you use?	Yes/No	Per organization. Only applicable if you have an asset register.
5.8 Do you record cyber security incidents?	Yes/No	Per organization.
5.9 Upload documented cyber security incidents(s)	File upload	Per organization.
5.10 Do you have a cyber security incident response plan?	Yes/No	Per organization.
5.11 Do you have a digital copy of your cyber security incident response plan?	Yes/No	Per organization.
5.12 Upload incident response plan(s)	File upload	Per organization.

5.13	How often do you exercise the incident response plan?	Selection	Per organization. Annually, less or never
5.14	Do you have a cyber security response team?	Selection	Per organization. Internal, External or Both
5.15	Name/Provider for external cyber security response team	Text input	Per organization. Only applicable if you have an external cyber security response team
5.16	During the policy period, which cyber security response team do you want to use?	Selection	Per organization. DNK or Retained
5.17	Do you have any policies outlining procedures and account verification before making payments?	Yes/No	Per organization.
5.18	When was the last time you conducted a cyber vulnerability assessment or penetration test?	Date	Per organization. DD/MM/YYYY
5.19	Do you conduct cyber security awareness training?	Selection	Per organization. Annually, less or never.
5.20	Do you employ backup and/or Disaster Recovery?	Selection	Per organization. Backup, Disaster Recovery or Both
5.21	Has your backup been tested?	Yes/No	Per organization. Only applicable if you employ backup.
5.22	Has the Disaster Recovery been tested?	Yes/No	Per organization. Only applicable if you employ Disaster Recovery.
5.23	Do you actively monitor, patch and update all software/firmware used on devices within the organisation?	Yes/No	Per organization.
5.24	Do you use on-premises servers?	Yes/No	Per organization.
5.25	Which type of firewalls or intrusion detection systems does the company employ?	Text input.	Per organization. Only applicable if you use on-premises servers.
5.26	Do you employ any endpoint detection (EDR) and/or antivirus on company devices?	Yes/No	Per organization.
5.27	Name / Provider for EDR	Text input.	Per organization. Only applicable if employ Endpoint detection.
5.28	Do you employ a Security Operations Center?	Selection	Per organization. Internal, External or Both
5.29	Name / Provider for external SEC	Text input.	Per organization. Only applicable if you employ an external Security Operations Center.
5.30	Does your company use cloud based e-mail services?	Selection	Per organization. Microsoft, Google, AWS or other.

5.32	Do you log network activity, application activity or Active Directory access(AD)?	Checkbox	Per organization. Network, application and/or Active Directory
5.33	Do you employ Multi Factor Authentication (MFA) access for remote access to the corporate data, systems, applications or infrastructure?	Yes/No	Per organization.
5.34	Are there any exemptions? (systems/applications where MFA is not employed)	Text input	Per organization. Only applicable if you employ MFA for for remote access.
5.35	Do you employ access control measures for your data?	Yes/No	Per organization.
5.36	Does the company store or process Special Categories of Personal Data or Payment Card Information (PCI)?	Checkbox	Per organization. Special Personal Data or Payment Card Information.
5.37	Has your company performed a Data Protection Impact Assessment (DPIA)?	Yes/No	Per organization. See Datatilsynet .
5.38	Upload documentation for DPIA	File upload	Per organization.

6. Supply chain and managed services

Question	Type	Description
6.1 Do your contracts with your Key Suppliers regulate requirements and responsibility for cyber security measures?	Yes/No	
6.2 Do you regularly conduct cyber security assessments of your Key Suppliers (questionnaire, audit, pen test or similar)?	Yes /No	
6.3 Do you use a Managed Service Provider for your IT services?	Yes/No	
6.4 Help desk support, troubleshooting and issue resolution, network management, server maintenance, and more	Yes/No	Only applicable if you use Manages Service Provider for IT services
6.5 Vulnerability assessments, penetration testing, threat monitoring and detection, incident response, and disaster recovery planning.	Yes/No	Only applicable if you use Manages Service Provider for IT services
6.6 Manage cloud-based applications and services, such as Office 365, Google Workspace, or cloud-based storage solutions.	Yes/No	Only applicable if you use Manages Service Provider for IT services
6.7 Backup and recovery solutions to ensure that critical data and systems are protected from loss or damage.	Yes/No	Only applicable if you use Manages Service Provider for IT services
6.8 Technology infrastructure, such as servers, network devices, and storage systems, ensuring they are up-to-date, optimized, and secure.	Yes/No	Only applicable if you use Manages Service Provider for IT services
6.9 Are you contractually liable to access and audit data from your MSP(s)?	Yes/No	Only applicable if you use Manages Service Provider for IT services

7. Vessel maturity

Question	Type	Description
7.1 Confirm names of insured vessels	Yes/No	Per vessel
7.1.1 Vessel names/IMO number	Yes/No	Per vessel
7.1.2. Cyber secure class notation (DNV) (Or planned?)	Yes/No	Per vessel
7.1.3 Starlink or similar technology implemented? (Or planned)	Yes /No	Per vessel
7.2 Is Starlink or similar technology used for operationally critical IT/OT?	Yes/No	
7.3 If Starlink used, do you have any preventive measures in place to avoid misuse?	Yes/No	
7.4 Do you have cyber security policy for your fleet?	Yes/No	
7.5 How often do you update the cyber security policy for the fleet?	Selection	Annually, less or never
7.6 Cyber training and exercise on vessels?	Selection	Annually, less or never

8. Key Service Providers

Question	Type	Description
8.1 Provider	List	List all providers
8.2 System(s)	List	List all systems
8.3 Deployments	Select	Select what subsidiaries and vessels systems listed are deployed
8.3.1 Deployed at subsidiaries	Select	Select what subsidiaries systems listed are deployed
8.3.2 Deployed on vessels	Select	Select what vessels systems listed are deployed

9. Additional information

Question	Type	Description
9.1 Additional disclosures?	Text input	
9.2 Upload additional files	File upload	