Development of Maritime Cybersecurity Protocols Report

Project Acronym:	CyberSEA
Full Title:	CyberSEA - Increasing Cyber Security at SEA through digital training
Project no.:	2023-1-ES01-KA220-VET-000159793
File Ref:	WP2T5 Development of Maritime Cybersecurity Protocols
Version:	1.0
Status:	Final
Start date of the project:	01.09.2023 ***Duration:*** 36 months
Dissemination level:	RE: Restricted to a group specified by the consortium (including the national agency services)
Funding body:	Co-funded by the European Union
Partners' logo:	

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

List of CyberSEA Beneficiaries

No.	Participant Organisation Name	Participant Short Name	Country
1	UNIVERSITAT POLITECNICA DE CATALUNYA	UPC	ES
2	AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA	IDEC	GR
3	SPINAKER, navticno izobrazevanje in trgovina, d.o.o.	SPINAKER	SI
4	Academia Navala "Mircea cel Batran"	RNA	RO
5	Berlin School of Business and Innovation GmbH	BSBI	DE
6	Centre for Factories of the Future	C4FF	SE
7	POLITECHNIKA MORSKA W SZCZECINIE PM	MUS	PL
8	ELLINIKO MESOGEIAKO PANEPISTIMIO	HMU	GR
9	SATAKUNNAN AMMATTIKORKEAKOULU OY	SAMK	FI

List of Output Contributors

No.	Participant Organisation Name	Participant Short Name	Country
1	UNIVERSITAT POLITECNICA DE CATALUNYA	UPC	ES
2	AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA	IDEC	GR
3	SPINAKER, navticno izobrazevanje in trgovina, d.o.o.	SPINAKER	SI
4	Academia Navala "Mircea cel Batran"	RNA	RO
5	Berlin School of Business and Innovation GmbH	BSBI	DE
6	Centre for Factories of the Future	C4FF	SE
7	POLITECHNIKA MORSKA W SZCZECINIE PM	MUS	PL
8	ELLINIKO MESOGEIAKO PANEPISTIMIO	HMU	GR
9	SATAKUNNAN AMMATTIKORKEAKOULU OY	SAMK	FI

Contents

1. Passenger and Crew Management Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol aims to establish standardized procedures, guidelines, and measures to safeguard digital assets, systems, and operations from cyber threats, including SQL injection, phishing, Denial of services (DoS), and man in the middle (MITM) attacks. The protocol ensures resilience against these evolving cyber threats.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all digital systems, databases, networks, and operational platforms like **crew and passenger systems** that are susceptible to SQL injection, phishing attempts, denial of service attacks, and MITM interceptions. It covers both onboard and shore-based IT infrastructure.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	This protocol adheres to the following standards and regulations: IMO Guidelines on Maritime Cyber Risk Management
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Cybersecurity Officer: Oversees system monitoring and response to SQL injection, phishing, DoS, and MITM attacks. • IT Administrators: Ensure regular security updates, including protection against SQL injection vulnerabilities in databases, DoS mitigation tools, and network encryption for MITM attack prevention. • Employees and Crew Members: Follow best practices to avoid phishing attempts and report any suspicious activities. • External Auditors: Perform cybersecurity assessments focusing on vulnerabilities related to SQL injection, DoS attacks, and encryption standards for MITM.

Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	• Systematic Scanning: Utilize advanced scanning software to regularly assess digital systems, networks, and applications for vulnerabilities that could be exploited by cyber threats. This includes scanning for both known vulnerabilities and unusual system behaviors that might indicate emerging threats. • External Audits: Engage with third-party cybersecurity experts to conduct external audits of the maritime operations' cybersecurity practices. These audits provide an objective review of the current security measures and identify potential areas for improvement.
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** • Role-Based Access Control (RBAC): Implement RBAC to ensure that access to systems is based on the user's role within the organization, limiting the exposure of sensitive systems and data. • Multi-Factor Authentication (MFA): Enforce MFA for all critical systems to significantly reduce the risk of unauthorized access.
	Data Protection • Parameterized Queries: Utilize parameterized queries for all database interactions to eliminate the risk of SQL injection. • Data Encryption: Encrypt sensitive data both at rest and in transit to secure information from unauthorized interception and access.
	System Security • Regularly patch systems to close vulnerabilities that could lead to SQL injection or DoS attacks.

	• Secure web applications by regularly testing against SQL injection using penetration testing. • Deploy email filtering systems to detect phishing emails. • Educate employees on identifying phishing attempts and enforce strict policies regarding email attachments and links.
	Network Security • End-to-End Encryption: Apply strong encryption protocols to all data transmissions to protect data integrity and confidentiality against interception. • Intrusion Detection Systems (IDS): Use IDS to monitor for signs of an impending or ongoing attack, especially for high volumes of traffic that could indicate a DoS attack.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** • Use monitoring tools to detect anomalies such as large amounts of traffic (indicating DoS), unauthorized access attempts (MITM), or abnormal database queries (SQL injection). • Rapid Response Teams: Designate and train rapid response teams for different types of cyber incidents to ensure quick and effective handling of potential breaches.
	Incident Reporting • Automated Alerting Systems: Utilize automated systems to ensure that any anomalous activity is immediately reported to the cybersecurity team for rapid assessment.
	Incident Containment • System Isolation and Quarantine: Quickly isolate and quarantine affected systems or network segments. This includes disconnecting databases and systems

	from the network, ensuring that the threat does not spread and minimizing the impact on unaffected areas. • Traffic Control and Filtering: Use firewalls and intrusion prevention systems to control, filter, and reroute network traffic to and from compromised systems. This helps prevent the escalation of the incident and protects critical network infrastructure from further exposure. • Access Control Adjustments: Temporarily tighten access controls and disable or modify user accounts that are suspected of being compromised. This step is crucial to securing the network against unauthorized access and preventing further exploitation of system vulnerabilities. • Secure Communication Channels: Re-establish and secure communication channels to ensure that response teams can coordinate effectively without risking further exposure. Replace any compromised security certificates to maintain the integrity of data transmissions. • Backup Activation and System Restoration: Activate standby systems or revert to secure backups to maintain operational continuity. This ensures that essential functions remain online while primary systems are being cleansed and restored.
	Post-Incident Recovery • System Recovery and Validation: Prioritize the restoration of affected systems by ensuring that they are thoroughly cleaned and restored to their original state. Validate the integrity and functionality of the systems before

	bringing them back online to ensure they are free from any threats. • Data Restoration: Carefully restore data from backups after verifying that the backups are free of any malicious alterations. Implement strict validation processes to ensure that all restored data maintains its integrity and confidentiality. • Root Cause Analysis: Conduct a comprehensive root cause analysis to determine the specific vulnerabilities that were exploited and the origin of the incident. • Security Enhancements: Based on the findings from the root cause analysis, implement necessary updates and enhancements to cybersecurity measures to prevent similar incidents. • Document all aspects of the incident response and recovery process for future reference and for compliance purposes. • Review and Training: Review the incident with key personnel and update training materials based on lessons learned. Conduct training sessions to ensure all relevant staff are aware of the new security measures and understand their roles in preventing future incidents.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Simulation-Based Training: Regularly conduct realistic simulation exercises to prepare staff for actual attack scenarios, emphasizing the importance of security practices and procedures. • Ongoing Security Education: Offer continuous education on emerging cybersecurity threats and defensive tactics to keep personnel updated and prepared.

	Cybersecurity Drills • Regularly Scheduled Drills: Conduct drills at regular intervals to test the effectiveness of both the technical and procedural aspects of the cybersecurity protocols. • Scenario-Based Training: Design and implement a variety of attack scenarios to challenge the readiness of the cybersecurity team and other relevant personnel. Scenarios should cover a wide range of potential threats, from data breaches to system intrusions and phishing attacks.
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Conduct both internal and external audits focusing on the detection and mitigation of SQL injection, DoS, MITM, and phishing risks. • Review system logs for signs of potential attacks, ensuring protocols are in place and functioning effectively.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Maintain a clear line of communication between onboard and shore-based personnel, especially in the event of phishing, DoS, or MITM attacks to ensure timely response and containment. • Secure communication channels must be in place to prevent interception by MITM attacks.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Conduct formal reviews of the cybersecurity protocols every six months to ensure they are up-to-date and effective against current cyber threats. • In addition to scheduled reviews, the protocols must be promptly reviewed and potentially updated in response to significant new cybersecurity incidents or news related to exploits affecting software and systems used within maritime operations.

Appendix Include additional resources or reference materials if applicable eg. list of contacts	

2. Satellite Communication Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol is specifically tailored to secure the **satellite communication** devices and transmission channels aboard ships. It aims to establish detailed procedures, standards, and guidelines to protect these critical systems from cyber threats, ensuring secure, reliable, and uninterrupted communications for navigation, emergency response, and operational management.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	The protocol applies to all aspects of shipboard **satellite communication infrastructure**, including: • VSAT (Very Small Aperture Terminal) systems for broadband and voice communication. • Satellite phones and services such as Inmarsat, Iridium, or Globalstar for voice and data services. • GNSS (Global Navigation Satellite System) receivers for positioning, navigation, and timing. • All interfaces and networks that connect SATCOM to shipboard and shore-based systems.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Guidelines on Maritime Cyber Risk Management, focusing on satellite communications. • ISO/IEC 27001 for information security management tailored to SATCOM environments. • NIST Cybersecurity Framework for structuring cybersecurity risk management. • ETSI TS 103 479 for SATCOM-specific cybersecurity standards.

	• ISO/IEC 27001 adapted for satellite communications, specifically for Inmarsat's infrastructure.
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Cybersecurity Officer: Oversees the overall security of SATCOM, manages incident response, and coordinates cybersecurity strategy. • IT/SATCOM Administrators: Ensure software and hardware security, manage updates, and monitor network integrity. • Bridge officers should regularly cross-check satellite-based positioning with alternative navigation sources such as Inertial Navigation Systems (INS), radar observations, and celestial navigation methods to detect GPS spoofing attempts. • Communication Officers: Responsible for the secure operational use of SATCOM, reporting anomalies. • External Security Consultants: Perform specialized audits and penetration testing.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	• Regular security updates – Keeping SATCOM software and firmware up to date. • Continuous network activity monitoring – Detecting unauthorized access attempts. • Data encryption – Preventing eavesdropping and data manipulation. • Redundant communication systems – Ensuring operational continuity with HF/VHF radio and secondary satellite channels. • Access control mechanisms – Restricting modifications to SATCOM settings to authorized personnel. • Navigation Message Authentication (NMA) – Enhancing GPS integrity. • Cross-verification of navigation data – Using multiple sources to detect spoofing. • Signal strength monitoring – Identifying potential jamming or interference attempts.

Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Device Security** • Physical Security: Secure placement of SATCOM antennas and equipment to prevent physical tampering. • Firmware Security: Regular updates to satellite modem firmware to address known vulnerabilities, with secure boot processes to ensure integrity.
	Transmission Security • Encryption: Implement end-to-end encryption for all SATCOM transmissions, using standards like AES (Advanced Encryption Standard) for data confidentiality. • Signal Integrity: Use anti-jamming technologies and signal authentication to protect against interception or manipulation of satellite signals.
	Network Security • Firewall Configuration: Tailor firewalls to handle the unique aspects of satellite communication protocols, including managing bandwidth and latency. • Intrusion Detection: Use IDS tailored for satellite link characteristics to detect unauthorized access or anomalies in transmission patterns.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** • Anomaly monitoring – Identifying unusual traffic, performance degradation, or interference. • Data integrity validation – Cross-checking SATCOM messages with HF/VHF reports. • GPS signal integrity verification – Comparing current positions with past readings.
	Incident Reporting • Immediate escalation – Promptly notifying the Cybersecurity Officer of detected threats.

	• Incident categorization – Classifying events by severity and impact.
	Incident Containment • Immediate steps to secure affected SATCOM devices, potentially redirecting communications to alternative satellite paths or backup systems. • System isolation – Preventing unauthorized access from spreading within networks. • Account suspension – Disabling compromised credentials.
	Post-Incident Recovery • Secure restoration – Reloading SATCOM configurations from verified backups. • Integrity checks on all transmissions • Identifying root causes to prevent recurrence. • Security protocol updates – Implementing lessons learned to improve future resilience.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Simulation-Based Training: Regularly conduct realistic simulation exercises to prepare staff for actual attack scenarios, emphasizing the importance of security practices and procedures. • SATCOM Security Workshops: Training specifically on securing satellite equipment, understanding signal security, and recognizing transmission anomalies.
	Cybersecurity Drills • Before embarking on voyages, crew members and officers should receive briefings on SATCOM cybersecurity best practices, current threat landscapes, and emergency response procedures. • Education on cyber threats – Training personnel on GPS spoofing, jamming, and phishing tactics.

	• Backup communication training – Familiarizing crew with HF/VHF alternatives
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Log review protocols – Analyzing network traffic for signs of cyber threats. • Performance validation – Verifying SATCOM functionality and resilience against interference. • SATCOM-Specific Audits: Quarterly internal reviews focusing on device security, software/firmware updates, and signal transmission integrity. • Annual External Review: Comprehensive audit by specialists in satellite communications cybersecurity.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Establish a dedicated communication channel for SATCOM cybersecurity alerts, ensuring rapid response and coordination with satellite service providers. • A dedicated, secure reporting mechanism (e.g., an encrypted email system, a secure web portal, or a blockchain-based logging system) should be established for maritime stakeholders to report cyber threats or suspected incidents in real time. • End-to-End Encryption – All SATCOM-related communications, including operational messages, navigational data, and cybersecurity alerts, must be encrypted to prevent eavesdropping or data interception. Modern encryption protocols such as AES-256 or TLS 1.3 should be implemented to secure both data at rest and data in transit. • Controlled Use of Public Networks – Crew members should be trained to differentiate between operational SATCOM communications and personal or non-essential data usage. Critical SATCOM operations should be isolated from

	unsecured public networks to prevent unauthorized access. • Ship-to-Shore Cybersecurity Synchronization – Onboard IT and SATCOM security personnel must maintain a continuous exchange of information with shore-based cybersecurity teams. This includes real-time monitoring of network traffic, incident alerts, and compliance reporting. • Coordination with National and International Authorities – Maritime SATCOM operators should have predefined protocols for reporting cyber incidents to international bodies like the International Maritime Organization (IMO), International Telecommunications Union (ITU), and national cybersecurity agencies. This facilitates coordinated efforts in responding to large-scale cyber threats affecting multiple vessels or ports.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Biannual Protocol Reviews that should assess: -Evaluating reports from cybersecurity agencies (e.g., ENISA, NIST, IMO, ITU) to update defensive measures against new cyberattack techniques such as AI-powered malware, quantum decryption threats, and deepfake-based social engineering. - Regulatory Compliance Updates: - Technological Advancements: Incorporating improvements in encryption standards, firewall technologies, intrusion detection systems (IDS), and satellite communication hardening to maintain robust cybersecurity defenses. • Immediate Updates Following Cyber Incidents or Security Advisories
Appendix	

Include additional resources or reference materials if applicable eg. list of contacts	

3. Weather Monitoring Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol establishes standardized procedures, guidelines, and measures to safeguard **Weather Monitoring Systems** (WMS) onboard ships from cyber threats. These systems are vital for navigation, safety, and operational planning. Ensuring their protection from unauthorized access, malware infections, GPS spoofing, jamming, and data manipulation maintains the accuracy and reliability of weather data at sea.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all digital weather monitoring equipment, including: • Onboard weather stations • Satellite-based meteorological data receivers • Automated weather reporting systems • Associated networks and databases It covers both onboard and shore-based IT infrastructure supporting WMS operations.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Guidelines on Maritime Cyber Risk Management • ISO/IEC 27001: Information Security Management • NIST Cybersecurity Framework • International Safety Management (ISM) Code
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Cybersecurity Officer: Monitors and responds to cyber threats affecting WMS. • IT Administrators: Maintain security patches, monitor traffic, and prevent unauthorized access. • Bridge Officers & Crew: Observe best practices, report anomalies, and verify WMS data. • External Auditors: Conduct cybersecurity assessments on WMS vulnerabilities.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with	• Regular vulnerability scans of WMS software and hardware • Monitoring network activity for unauthorized access attempts

cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	• Secure backups of weather data stored on independent systems • Redundant weather data sources (e.g., shiptraffic.net, marine.meteoconsult.co.uk, oceanweather.com, accuweather.com)
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** • Role-Based Access Control (RBAC) to restrict WMS access: Implement RBAC to ensure that access to systems is based on the user's role within the organization, • Multi-Factor Authentication (MFA) for remote access to weather data servers to significantly reduce the risk of unauthorized access
	Data Protection • Encrypt weather data in transit and at rest • Use digital signatures to verify meteorological data authenticity • Use authentication protocols to prevent unauthorized weather data modifications
	System Security • Apply timely security patches and software updates • Monitor and reset systems if weather data appears manipulated • Verify onboard sensors to ensure they are functioning correctly
	Network Security • Firewalls & Intrusion Detection Systems (IDS) to monitor traffic,, especially for high volumes of traffic that could indicate a DoS attack. • Segregation of WMS networks from other onboard IT systems • Analyze system logs for unusual weather data modifications
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond,	**Incident Detection** • Monitor for anomalies, including unusual data transmissions or unexpected GPS behavior

contain, and recover from an attack.	• Cross-check WMS data with visual observations, radar, and external satellite sources • Detect signal jamming affecting weather data reception
	Incident Reporting • Immediate reporting of cybersecurity incidents to the Cybersecurity Officer • Document and categorize incidents based on severity
	Incident Containment • Isolate affected systems to prevent data tampering from spreading • Disable autopilot if discrepancies between real-world weather and system data arise • Inspect physical weather sensors to rule out tampering
	Post-Incident Recovery • Restore data from backups after validating integrity • Investigate root causes to prevent future incidents • Update security protocols based on lessons learned • Cross-check alternative sources (e.g., Inmarsat, NAVTEX) to verify weather reports
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Simulation-Based Training: Regularly conduct realistic simulation exercises to prepare staff for actual attack scenarios, emphasizing the importance of security practices and procedures. • Ongoing Security Education: Offer continuous education on emerging cybersecurity threats and defensive tactics to keep personnel updated and prepared.
	Cybersecurity Drills • Design and implement a variety of cyber incidents affecting WMS (scenario based training) to challenge the readiness of the

	cybersecurity team and other relevant personnel. • Education of crew personnel on manual weather observations (barometric pressure, wind patterns) to validate digital forecasts • Build awareness of social engineering tactics used to manipulate weather data
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Conduct both internal and external audits focusing on the detection and mitigation, especially of unauthorized access, malware infections, sensors reading or other weather data manipulation • Review system logs for signs of potential attacks, ensuring protocols are in place and functioning effectively.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Maintain a clear line of communication between onboard and shore-based personnel • Establish secure communication channels for reporting and responding to cybersecurity incidents
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Biannual reviews of cybersecurity protocols for WMS • In addition to scheduled reviews, the protocols must be promptly reviewed and potentially updated in response to significant new cybersecurity incidents or news related to exploits affecting software and systems used within maritime operations.
Appendix Include additional resources or reference materials if applicable eg. list of contacts	

4. Navigation Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol establishes standardized procedures, guidelines, and measures to safeguard **Bridge Navigation System** onboard ships from cyber threats. These systems are vital for navigation, safety, and operational planning. Ensuring their protection from unauthorized access, malware infections, GPS spoofing, jamming, and data manipulation maintains the accuracy and reliability of vessel navigation at sea.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all onboard navigation equipment, including: • ECDIS (Electronic Chart Display and Information System) • RADAR (Radio Aided Detection And Ranging) • Position sensors (Differential GPS) • Heading sensors (gyro compasses) • Automatic Identification System (AIS) • Integrated alarm system (IAS)
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Cybersecurity Guidelines (MSC-FAL.1/Circ.3) • ISPS Code (International Ship and Port Facility Security)-external threats towards with we can only prepare. • SOLAS (Safety of Life at Sea) • ISM Code (Internation Safety Management)-internal threats emerging from our actions. • SSP (Ship Security Plan) as required in the ISPS Code. • SMS (Safety Management System) as required in the ISM Code. • BIMCO (Baltic and International Marine Council) Guidelines on Cyber Security – Industry best practices for ships. • NIST (National Institute of Standards and Technology) Cybersecurity Framework –

	International best practices for data protection.
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• SSO (Ship Security Officer) responsible for implementing and maintaining the Ship Security Plan (SSP) • CSO (Company Security officer) • DPA (Designated Person Ashore) to collaborate with the vessel management team to support the implementation of Safety management System. • Duty deck officer: Observe best practices, report anomalies, and verify navigation data using multiple information sources. • Watchkeeper: Report anomalies to duty deck officer. • Internal auditor: Ensure the established SSP is followed as intended. • External auditor: Ensure the vessel and the managing company are in line with the international regulations and flag state legislation.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	Identifying Navigation Hazards • Shallow waters Risk of grounding • Traffic congestion High density of vessels increasing collision risks. • Adverse weather Storms, fog, or heavy rain affecting visibility. • Malfunctioning navigation equipment GPS failure, radar issues, or ECDIS errors. • Cyber threats GPS spoofing, AIS hacking, or electronic chart manipulation. Assessing Risk Severity & Likelihood • Likelihood (rare to frequent) • Impact (minor to catastrophic) • Risk Level (low, medium, high)

Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** • Implementing Risk Control Measures • Once risks are identified, mitigation strategies should be applied: • Passage Planning (Berth to Berth Planning) Proper use of ECDIS, paper charts, and waypoints. • Bridge Resource Management (BRM) Effective teamwork, decision-making, and communication. • Regular Equipment Checks Ensuring radar, AIS, GPS, and other navigational tools are operational. • Vessel Traffic Services (VTS) Coordination Following port and coastal traffic guidelines. • Contingency Planning Preparing for emergencies like loss of propulsion, steering failures, or sudden fog. Navigation risks constantly change due to weather, traffic, trading areas, mechanical issues and electronic issues. Therefore, the onboard watchkeepers must regularly practice cyclic risk assessment. This includes, but is not limited to, following actions. • Continuously monitor AIS, Radar, and ECDIS for real-time data. • Reflect the ECDIS information to that provided by the radar. • Do not rely on AIS targets in decision making. • Always use ARPA function with the radar. • Compare 3cm and 10cm radar information. • Adjust passage plans when new risks arise. • Communicate changes with the crew and bridge team.

	Data Protection Navigation data protection is critical to ensuring the security, reliability, and integrity of shipboard navigation systems. With increasing digitalization in the maritime industry, protecting navigation data from cyber threats, unauthorized access, and system failures is essential for safe voyages.
	System Security • Use encrypted communication as far as possible • Protect AIS and VHF data from interception. • Enable Multi-Factor Authentication (MFA) • Restrict access to critical systems. • Install Software Updates & Patches • Prevent vulnerabilities in ECDIS and GPS. • Segregate networks • Separate operational (OT) and IT networks to prevent cyber intrusions. • Monitor for anomalies • Regularly check for inconsistencies in AIS and GPS data. • Backup navigational data • Store offline backups of ECDIS and route plans.
	Network Security • Segregate Networks • Separate operational (OT) and IT networks to prevent cyber intrusions.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** Network & System Monitoring ● Intrusion Detection Systems (IDS) Identifies unauthorized network access. ● Security Information and Event Management (SIEM) Analyzes logs for suspicious activity. ● Endpoint Protection Software Detects malware and abnormal behavior on shipboard devices.

	• Network Traffic Analysis (NTA) Monitors data flow for unusual patterns. Anomaly Detection and Behavior Analysis • Working culture Establish protocols for using ship networks and systems. • GPS and AIS data verification Cross-check navigation data from multiple sources. Log keeping and Auditing • Review Access Logs Detect unauthorized login attempts. • Monitor Software Changes Identify unauthorized software installations or system modifications. • Regular Cybersecurity Audits • Assess vulnerabilities and compliance.
	Incident Reporting As required by IMO MSC-FAL.1/Circ.3 Submit an incident report form to at least: • Company Security Officer (CSO) • Flag state authorities • Port Facility Security Officer (PFSO) (if in port) Classification society
	Incident Containment • Conduct forensic investigation to determine the root cause. • Assess the extent of the breach and potential data loss. • Identify weaknesses and propose corrective measures. **Post-Incident Recovery** • Update cybersecurity policies and response procedures.

	• Conduct crew training to improve awareness and response skills. • Enhance security controls (firewalls, access controls, software updates). • Report lessons learned to IMO, classification societies, and stakeholders. • Restore affected systems from secure backups. • Apply security patches and software updates. • Strengthen firewall and access controls. • Conduct crew cybersecurity training to prevent future attacks. • Update Risk Management Plan following the IMO MSC-FAL.1/Circ.3.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** Navigation • Chartwork Using paper charts, gyro- and magnetic compass radar fixes. • Dead Reckoning & Position Fixing Estimating position based on speed and course. • Electronic Chart Display and Information System (ECDIS) Chart usage. • Global Positioning System (GPS/GNSS) Satellite-based positioning. • Automatic Identification System (AIS) Ship tracking and collision avoidance. • Radar & ARPA (Automatic Radar Plotting Aid) Identifying obstacles and traffic. Bridge Resource management • Situational awareness • Monitoring surroundings for safe navigation. • Team communication • Effective watchkeeping and leadership. • Decision-making under pressure

	• Responding to sudden emergencies
	Cybersecurity Drills Theory-based training • Understanding maritime regulations (IMO, STCW, SOLAS). • Learning navigational chart symbols, buoyage systems, and passage planning. Simulator Training • ECDIS and radar simulation Practicing real-world scenarios. • Collision avoidance drills Simulating encounters with other vessels. • Emergency navigation exercises • Responding to GPS failures or cyber threats. Onboard training • Hands-on experience with shipboard navigation equipment. • Practicing lookout duties and safe bridge operations. • Performing real-time passage planning and execution.
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Follow IMO MSC-FAL.1/Circ.3 (Cyber Risk Management Guidelines) • Auditing framework is entirely dictated by the IMO ISPS Code. • Internal auditing and external auditing annually.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	Collect Incident Information • Date time When was the incident first detected? When did it occur? • Location Ship's position (latitude/longitude) or port location. • Type of incident

	Malware, phishing, unauthorized access, GPS spoofing, etc. ● Systems affected Navigation, communications, IT network, cargo handling, alarm systems, weather monitoring, etc. ● Threat origin Suspicious emails, external access, unknown software, etc. ● Response actions Steps taken to mitigate consequences or to contain the hazard. ● Reporting Report to (does not overrule company SMS protocol): ● Company Security Officer (CSO) ● Flag state authority ● Port Facility Security Officer (PFSO-when moored or at anchor) ● Ships agent Classification society (if required)

Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	Follow IMO MSC-FAL.1/Circ.3 (Cyber Risk Management Guidelines) The management review is designed to assess the effectiveness of the SMS and ensure it is functioning as intended. It is conducted periodically to: ● Evaluate performance – Ensure safety procedures are being followed and are effective. ● Identify non-conformities – Recognize areas where the SMS needs improvement. ● Ensure compliance – Verify that the SMS complies with regulatory requirements and industry best practices. ● Promote continual improvement – Support a culture of ongoing safety and quality improvement. ● Review of SMS Effectiveness ● Non-conformities, Corrective and Preventive Actions ● Accident and Incident Reports ● Legal and Regulatory Compliance ● Continuous Improvement
Appendix Include additional resources or reference materials if applicable eg. List of contacts	See the list in the regulations-paragraph.

5. Integrated Bridge Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol establishes standardized procedures, guidelines, and measures to safeguard **Integrated Bridge Systems (IBS)** onboard from cyber threats. These systems are vital for navigation, safety, and operational planning. Ensuring their protection from unauthorized access, malware infections, GPS spoofing, jamming, and data manipulation maintains the accuracy and reliability of vessel navigation at sea.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to IBS equipment, including all equipment involving one or more of the following: • Execution of passage • Communications • Machinery control • Cargo operations • Safety and security As per the IMO definition: “An integrated bridge system (IBS) is defined as a combination of systems which are interconnected in order to allow centralized access to sensor information or command/control from workstations, with the aim of increasing safe and efficient ship's management by suitably qualified personnel.” “INS evaluates input from sensors to provide warnings of dangers and degraded information. IBS allows centralized access to sensor information from workstations to increase safe ship management.”

Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Cybersecurity Guidelines (MSC-FAL.1/Circ.3) • ISPS Code (International Ship and Port Facility Security)-external threats towards with we can only prepare. • SOLAS (Safety of Life at Sea) • ISM Code (Internation Safety Management)-internal threats emerging from our actions. • SSP (Ship Security Plan) as required in the ISPS Code. • SMS (Safety Management System) as required in the ISM Code. • BIMCO (Baltic and International Marine Council) Guidelines on Cyber Security – Industry best practices for ships. • NIST (National Institute of Standards and Technology) Cybersecurity Framework – • International best practices for data protection.
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• SSO (Ship Security Officer) responsible for implementing and maintaining the Ship Security Plan (SSP) • CSO (Company Security officer) • DPA (Designated Person Ashore) to collaborate with the vessel management team to support the implementation of Safety management System. • Duty deck officer: Observe best practices, report anomalies, and verify navigation data using multiple information sources. • Watchkeeper: Report anomalies to duty deck officer. • Duty engineer: Report anomalies to duty deck officer. • Internal auditor: Ensure the established SSP is followed as intended. • External auditor: Ensure the vessel and the managing company are in line with the international regulations and flag state legislation.

Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	Identifying navigation hazards • Malfunctioning navigation equipment GPS failure, radar issues, or ECDIS errors. • Cyber threats GPS spoofing, AIS hacking, or electronic chart manipulation. Identify system level hazards • Technical systems. • Human operator. • Main-machine interface • Operational guidelines. Assessing risk-specific severity and likelihood • Likelihood (rare to frequent) • Impact (minor to catastrophic) • Risk Level (low, medium, high)
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	***Access Control*** • Implementing risk control measures • Once risks are identified, mitigation strategies should be applied: Navigation • Passage planning (berth to berth planning) Proper use of ECDIS, paper charts, and waypoints. • Bridge Resource Management (BRM) • Effective teamwork, decision-making and communication. • Regular Equipment Checks Ensuring radar, AIS, GPS, and other navigational tools are operational. • Vessel Traffic Services (VTS) Coordination Following port and coastal traffic guidelines. • Contingency Planning

	Preparing for emergencies like loss of propulsion, steering failures, or collision
	Navigation risks constantly change due to weather, traffic, trading areas, mechanical issues and electronic issues. Therefore, the onboard watchkeepers must regularly practice cyclic risk assessment. This includes, but is not limited to, following actions. • Continuously monitor AIS, Radar, and ECDIS for real-time data. • Reflect the ECDIS information to that provided by the radar. • Do not rely on AIS targets in decision making. • Always use ARPA function with the radar. • Compare 3cm and 10cm radar information. • Adjust passage plans when new risks arise. • Communicate changes with the crew and bridge team. Bridge systems ● Regular data comparison to ensure the used data remains the same from the source to the various equipment. ● IAS (Integrated Alarm System) provides alarms when needed. ● Engine control systems have no signal latency. ● Engine and propulsion setpoint- and feedback values are as expected. ● Comparison of conning system and the associated data in their various sources. ● VDR (Voyage Data Recorder) is free of anomalies and alarms. ● Steering equipment electronic panels have no alarms or latency. ● Change of control between control points function. ***Data Protection*** With increasing digitalization in the maritime industry, protecting vessel operational data from cyber threats,

	unauthorized access, and system failures is essential for safe voyages. ***System Security*** • Use encrypted communication as far as possible • Protect AIS and VHF data from interception. • Enable Multi-Factor Authentication (MFA) • Restrict access to critical systems. • Install Software Updates & Patches • Prevent vulnerabilities in ECDIS and GPS. • Segregate networks • Separate operational (OT) and IT networks to prevent cyber intrusions. • Monitor for anomalies • Regularly check for inconsistencies in AIS and GPS data. • Backup navigational data • Store offline backups of ECDIS and route plans. ***Network Security*** • Segregate Networks • Separate operational (OT) and IT networks to prevent cyber intrusions.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	***Incident Detection*** Network & System Monitoring ● Intrusion Detection Systems (IDS) – Identifies unauthorized network access. ● Security Information and Event Management (SIEM) – Analyzes logs for suspicious activity. ● Endpoint Protection Software – Detects malware and abnormal behavior on shipboard devices. ● Network Traffic Analysis (NTA) – Monitors data flow for unusual patterns.

	• Anomaly Detection and Behavior Analysis • Working culture • Establish protocols for using ship networks and systems. • Cross-check safety critical data from multiple sources. Log keeping and Auditing • Review Access Logs – Detect unauthorized login attempts. • Monitor Software Changes – Identify unauthorized software installations or system modifications. • Regular Cybersecurity Audits – Assess vulnerabilities and compliance. ***Incident Reporting*** As required by IMO MSC-FAL.1/Circ.3 Submit an incident report form to at least: • Company Security Officer (CSO) • Flag state authorities • Port Facility Security Officer (PFSO) (if in port) • Classification society ***Incident Containment*** • Conduct forensic investigation to determine the root cause. • Assess the extent of the breach and potential data loss. Identify weaknesses and propose corrective measures ***Post-Incident Recovery*** • Update cybersecurity policies and response procedures. • Conduct crew training to improve awareness and response skills. • Enhance security controls (firewalls, access controls, software updates). • Report lessons learned to IMO, classification societies, and stakeholders. • Restore affected systems from secure backups.

	● Apply security patches and software updates. ● Strengthen firewall and access controls. ● Conduct crew cybersecurity training to prevent future attacks. ● Update Risk Management Plan following the IMO MSC-FAL.1/Circ.3.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	***Training Programs*** Bridge Resource management ● Situational awareness Monitoring surroundings for safe navigation. ● Team communication Effective watchkeeping and leadership. ● Decision-making under pressure Responding to sudden emergencies
	Cybersecurity Drills Theory-based training ● Understanding maritime regulations (IMO, STCW, SOLAS). ● Learning navigational chart symbols, buoyage systems, and passage planning. Simulator Training ● Practicing real-world scenarios. ● Collision avoidance drills Simulating encounters with other vessels. ● Emergency exercises ● Responding to GPS failures or cyber threats. Onboard training ● Hands-on experience with shipboard bridge equipment. ● Practicing safe bridge operations.

Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Follow IMO MSC-FAL.1/Circ.3 (Cyber Risk Management Guidelines) • Auditing framework is entirely dictated by the IMO ISPS Code. • Internal auditing and external auditing annually.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	Collect Incident Information • Date time When was the incident first detected? When did it occur? • Location Ship's position (latitude/longitude) or port location. • Type of incident Malware, phishing, unauthorized access, GPS spoofing, etc. • Systems affected Navigation, communications, IT network, cargo handling, alarm systems, weather monitoring, etc. • Threat origin Suspicious emails, external access, unknown software, etc. • Response actions Steps taken to mitigate consequences or to contain the hazard. • Reporting Report to (does not overrule company SMS protocol): • Company Security Officer (CSO) • Flag state authority • Port Facility Security Officer (PFSO-when moored or at anchor) • Ships agent • Classification society (if required)

Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	Follow IMO MSC-FAL.1/Circ.3 (Cyber Risk Management Guidelines) The management review is designed to assess the effectiveness of the SMS and ensure it is functioning as intended. It is conducted periodically to: ● Evaluate performance ● Ensure safety procedures are being followed and are effective. ● Identify non-conformities ● Recognize areas where the SMS needs improvement. ● Ensure compliance Verify that the SMS complies with regulatory requirements and industry best practices. ● Promote continual improvement Support a culture of ongoing safety and quality improvement. ● Review of SMS Effectiveness ● Non-conformities, Corrective and Preventive Actions ● Accident and Incident Reports ● Legal and Regulatory Compliance ● Continuous Improvement
Appendix Include additional resources or reference materials if applicable eg. List of contacts	See the list in the regulations-paragraph.

6. Power Management Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol is specifically tailored to secure the **Power Management Systems**. It aims to establish detailed procedures, standards, and guidelines to protect these critical systems from cyber threats, ensuring secure, reliable, the normal operations and management of these critical systems that provide of electric energy to all systems of the ship as main propulsion, steering, navigation, etc.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	The protocol applies to the following systems: • Main Switch Board • Auxiliary engines
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Resolution MSC.428(98) • OCIMF SIRE 2.0 Inspection program • IACS Unified Requirements E26 and E7 • DNV class notation Cyber secure • EU NIS2 Directive • Country specific laws and requirements
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Owner o managing director as leaders agree on their roles and responsibilities in developing, implementation, and assessing the organization´s_ cybersecurity strategy. • Company IT manager will give support. • Ship IT manager (Master, Chief Mate and Marine Chief Engineer) will be responsible of ship IT infrastructure management. • Safety manager will give support • Procurement manager will give support • Fleet manager will give support • Marine human resources manager will be responsible of crew cyber risk management training

	• External Security Consultants: Perform specialized audits and penetration testing.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	**The four phases of a risk assessment** **Phase 1: Pre-assessment activities** • Assessment of cyber risks is a complex undertaking, which requires detailed knowledge about cyber risk management, and third-party support to the risk assessment process is likely to be required in some cases. • Prior to starting a cyber risk assessment on board, the following activities should be performed: • Review the documentation of IT and OT systems and assess potential impact levels. • Identify main manufacturers of critical shipboard IT and OT equipment (a risk-based approach should be used in this identification process). • Identify cyber security points-of-contact with the most important manufacturers and establish a working relationship with them. • Review detailed documentation on the ship's maintenance and support of the IT and OT systems. • Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment. **Phase 2: Ship assessment** When all risk factors (threats, vulnerabilities, likelihood and impact) are assessed, the risk assessment and associate risk mitigation can be carried out. The risk assessment is a systematic consideration of relevant risk factors. **Phase 3: Debrief and reporting** To satisfy the requirements of the ISM Code, the risk assessment should be a coherent and up-to date document which reflect how risks are assessed and mitigated.

	An initial third-party cyber risk assessment could for example include the following: • Executive summary – a high-level summary of results, recommendations, and the overall security profile of the assessed ship • technical findings – breakdown of discovered vulnerabilities, their probability of exploitation, the monetary cost of exploitation, the resulting impact on the crew, ship and environment, and appropriate technical fix and mitigation advice • prioritised list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list should be a complete list of options available and not represent a list of services and products, which the third party risk assessor, if applicable, would like to sell. • supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing, if any, of critical or high-risk vulnerabilities **Phase 4: Manufacturer's debrief** • Once the shipowner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the manufacturers of the effected systems in order to reduce or mitigate the risk. **Threat Identification:** To identify the threat, companies should consider any specific aspects of potential threat actors 'capability, opportunity, and intent of attack. The attack can be made by accidental actors, activists, including disgruntled employees, criminals, opportunists, States, State sponsored organizations and terrorists.

Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** The Access control should include the following security measurement: • physical security of the ship in accordance with the ship security plan (SSP) • protection of networks, including effective segmentation • intrusion detection • use of firewall • periodic vulnerability scanning and testing • software whitelisting • access and user controls • configuration and change management controls appropriate procedures regarding the use of removable media and password policies • personnel's cyber security awareness and understanding of the risk to themselves and the industry • understanding and familiarity with appropriate procedures, including incident response. **Data Protection** • Limitation to and control of network ports, protocols and services • Configuration of network devices such as firewalls, routers and switches **System Security** • Encryption: Implement end-to-end encryption for all SATCOM transmissions, using standards like AES (Advanced Encryption Standard) for data confidentiality. • Signal Integrity: Use anti-jamming technologies and signal authentication to protect against interception or manipulation of satellite signals. **Network Security** • Firewall Configuration: Tailor firewalls to handle the unique aspects of satellite communication protocols, including managing bandwidth and latency.

	• Intrusion Detection: Use IDS tailored for satellite link characteristics to detect unauthorized access or anomalies in transmission patterns.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** In accordance with ISM Code Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents. **Incident Reporting** In accordance to ISM Code, it must implement the following measures: • Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems. • Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence. • Update the specific measures aimed at promoting the reliability of OT. **Incident Containment** • Immediate steps to secure affected SATCOM devices, potentially redirecting communications to alternative satellite paths or backup systems. • System isolation – Preventing unauthorized access from spreading within networks. • Account suspension – Disabling compromised credentials. **Post-Incident Recovery** • Secure restoration – Reloading SATCOM configurations from verified backups. • Integrity checks on all transmissions • Identifying root causes to prevent recurrence. • Security protocol updates – Implementing lessons learned to improve future resilience. • Creation and maintenance of back-ups into the ship's operational maintenance routine.

Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization´s non-public resources • Train users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials) • Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole **Cybersecurity Drills** • Periodically assess or test users on their understanding of basic cybersecurity practices • Require annual refreshers to reinforce existing practices and introduce new practices • Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data • Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties • Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles • Require annual refreshers to reinforce existing practices and introduce new practices
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both	• Log review protocols – Analyzing network traffic for signs of cyber threats. • Performance validation – Verifying SATCOM functionality and resilience against interference.

internal and external audits and the frequency of such reviews.	• SATCOM-Specific Audits: Quarterly internal reviews focusing on device security, software/firmware updates, and signal transmission integrity. • Annual External Review: Comprehensive audit by specialists in satellite communications cybersecurity.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Establish a dedicated communication channel for SATCOM cybersecurity alerts, ensuring rapid response and coordination with satellite service providers. • A dedicated, secure reporting mechanism (e.g., an encrypted email system, a secure web portal, or a blockchain-based logging system) should be established for maritime stakeholders to report cyber threats or suspected incidents in real time. • End-to-End Encryption – All SATCOM-related communications, including operational messages, navigational data, and cybersecurity alerts, must be encrypted to prevent eavesdropping or data interception. Modern encryption protocols such as AES-256 or TLS 1.3 should be implemented to secure both data at rest and data in transit. • Controlled Use of Public Networks – Crew members should be trained to differentiate between operational SATCOM communications and personal or non-essential data usage. Critical SATCOM operations should be isolated from unsecured public networks to prevent unauthorized access. • Ship-to-Shore Cybersecurity Synchronization – Onboard IT and SATCOM security personnel must maintain a continuous exchange of information with shore-based cybersecurity teams. This includes real-time monitoring of network traffic, incident alerts, and compliance reporting. • Coordination with National and International Authorities – Maritime SATCOM operators

	should have predefined protocols for reporting cyber incidents to international bodies like the International Maritime Organization (IMO), International Telecommunications Union (ITU), and national cybersecurity agencies. This facilitates coordinated efforts in responding to large-scale cyber threats affecting multiple vessels or ports.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Biannual Protocol Reviews that should assess: -Evaluating reports from cybersecurity agencies (e.g., ENISA, NIST, IMO, ITU) to update defensive measures against new cyberattack techniques such as AI-powered malware, quantum decryption threats, and deepfake-based social engineering. - Regulatory Compliance Updates: - Technological Advancements: Incorporating improvements in encryption standards, firewall technologies, intrusion detection systems (IDS), and satellite communication hardening to maintain robust cybersecurity defenses. • Immediate Updates Following Cyber Incidents or Security Advisories
Appendix Include additional resources or reference materials if applicable eg. list of contacts	

7. Propulsion and Engine Control Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol is specifically tailored to secure the **Propulsion and Engine Control Systems**. It aims to establish detailed procedures, standards, and guidelines to protect these critical systems from cyber threats, ensuring secure, reliable, the normal operations and management of these critical systems
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	The protocol applies to the following systems: • Main engines propulsion • Auxiliary engines • Steering gear
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Resolution MSC.428(98) • OCIMF SIRE 2.0 Inspection program • IACS Unified Requirements E26 and E7 • DNV class notation Cyber secure • EU NIS2 Directive • Country specific laws and requirements
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Owner o managing director as leaders agree on their roles and responsibilities in developing, implementation, and assessing the organization´s_ cybersecurity strategy. • Company IT manager will give support. • Ship IT manager (Master, Chief Mate and Marine Chief Engineer) will be responsible of ship IT infrastructure management. • Safety manager will give support • Procurement manager will give support • Fleet manager will give support • Marine human resources manager will be responsible of crew cyber risk management training • External Security Consultants: Perform specialized audits and penetration testing.

Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	**The four phases of a risk assessment** **Phase 1: Pre-assessment activities** • Assessment of cyber risks is a complex undertaking, which requires detailed knowledge about cyber risk management, and third-party support to the risk assessment process is likely to be required in some cases. • Prior to starting a cyber risk assessment on board, the following activities should be performed: • Review the documentation of IT and OT systems and assess potential impact levels. • Identify main manufacturers of critical shipboard IT and OT equipment (a risk-based approach should be used in this identification process). • Identify cyber security points-of-contact with the most important manufacturers and establish a working relationship with them. • Review detailed documentation on the ship's maintenance and support of the IT and OT systems. • Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment. **Phase 2: Ship assessment** When all risk factors (threats, vulnerabilities, likelihood and impact) are assessed, the risk assessment and associate risk mitigation can be carried out. The risk assessment is a systematic consideration of relevant risk factors. **Phase 3: Debrief and reporting** To satisfy the requirements of the ISM Code, the risk assessment should be a coherent and up-to date document which reflect how risks are assessed and mitigated.

	An initial third-party cyber risk assessment could for example include the following: • Executive summary – a high-level summary of results, recommendations, and the overall security profile of the assessed ship • technical findings – breakdown of discovered vulnerabilities, their probability of exploitation, the monetary cost of exploitation, the resulting impact on the crew, ship and environment, and appropriate technical fix and mitigation advice • prioritised list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list should be a complete list of options available and not represent a list of services and products, which the third party risk assessor, if applicable, would like to sell. • supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing, if any, of critical or high-risk vulnerabilities **Phase 4: Manufacturer's debrief** • Once the shipowner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the manufacturers of the effected systems in order to reduce or mitigate the risk. **Threat Identification:** To identify the threat, companies should consider any specific aspects of potential threat actors 'capability, opportunity, and intent of attack. The attack can be made by accidental actors, activists, including disgruntled employees,

	criminals, opportunists, States, State sponsored organizations and terrorists.
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** The Access control should include the following security measurement: • physical security of the ship in accordance with the ship security plan (SSP) • protection of networks, including effective segmentation • intrusion detection • use of firewall • periodic vulnerability scanning and testing • software whitelisting • access and user controls • configuration and change management controls appropriate procedures regarding the use of removable media and password policies • personnel's cyber security awareness and understanding of the risk to themselves and the industry • understanding and familiarity with appropriate procedures, including incident response.
	Data Protection • Limitation to and control of network ports, protocols and services • Configuration of network devices such as firewalls, routers and switches
	System Security • Encryption: Implement end-to-end encryption for all SATCOM transmissions, using standards like AES (Advanced Encryption Standard) for data confidentiality. • Signal Integrity: Use anti-jamming technologies and signal authentication to protect against interception or manipulation of satellite signals.
	Network Security

	• Firewall Configuration: Tailor firewalls to handle the unique aspects of satellite communication protocols, including managing bandwidth and latency. • Intrusion Detection: Use IDS tailored for satellite link characteristics to detect unauthorized access or anomalies in transmission patterns.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** In accordance with ISM Code Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.
	Incident Reporting In accordance to ISM Code it must implementing the following measures: • Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems. • Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence. • Update the specific measures aimed at promoting the reliability of OT.
	Incident Containment • Immediate steps to secure affected SATCOM devices, potentially redirecting communications to alternative satellite paths or backup systems. • System isolation – Preventing unauthorized access from spreading within networks. • Account suspension – Disabling compromised credentials.
	Post-Incident Recovery • Secure restoration – Reloading SATCOM configurations from verified backups. • Integrity checks on all transmissions • Identifying root causes to prevent recurrence.

	• Security protocol updates – Implementing lessons learned to improve future resilience. • Creation and maintenance of back-ups into the ship's operational maintenance routine.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization´s non-public resources • Train users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials) • Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole
	Cybersecurity Drills • Periodically assess or test users on their understanding of basic cybersecurity practices • Require annual refreshers to reinforce existing practices and introduce new practices • Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data • Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties • Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles • Require annual refreshers to reinforce existing practices and introduce new practices

Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Log review protocols – Analyzing network traffic for signs of cyber threats. • Performance validation – Verifying SATCOM functionality and resilience against interference. • SATCOM-Specific Audits: Quarterly internal reviews focusing on device security, software/firmware updates, and signal transmission integrity. • Annual External Review: Comprehensive audit by specialists in satellite communications cybersecurity.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Establish a dedicated communication channel for SATCOM cybersecurity alerts, ensuring rapid response and coordination with satellite service providers. • A dedicated, secure reporting mechanism (e.g., an encrypted email system, a secure web portal, or a blockchain-based logging system) should be established for maritime stakeholders to report cyber threats or suspected incidents in real time. • End-to-End Encryption – All SATCOM-related communications, including operational messages, navigational data, and cybersecurity alerts, must be encrypted to prevent eavesdropping or data interception. Modern encryption protocols such as AES-256 or TLS 1.3 should be implemented to secure both data at rest and data in transit. • Controlled Use of Public Networks – Crew members should be trained to differentiate between operational SATCOM communications and personal or non-essential data usage. Critical SATCOM operations should be isolated from unsecured public networks to prevent unauthorized access. • Ship-to-Shore Cybersecurity Synchronization – Onboard IT and SATCOM security personnel must maintain a continuous

	exchange of information with shore-based cybersecurity teams. This includes real-time monitoring of network traffic, incident alerts, and compliance reporting. • Coordination with National and International Authorities – Maritime SATCOM operators should have predefined protocols for reporting cyber incidents to international bodies like the International Maritime Organization (IMO), International Telecommunications Union (ITU), and national cybersecurity agencies. This facilitates coordinated efforts in responding to large-scale cyber threats affecting multiple vessels or ports.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Biannual Protocol Reviews that should assess: -Evaluating reports from cybersecurity agencies (e.g., ENISA, NIST, IMO, ITU) to update defensive measures against new cyberattack techniques such as AI-powered malware, quantum decryption threats, and deepfake-based social engineering. - Regulatory Compliance Updates: - Technological Advancements: Incorporating improvements in encryption standards, firewall technologies, intrusion detection systems (IDS), and satellite communication hardening to maintain robust cybersecurity defences. • Immediate Updates Following Cyber Incidents or Security Advisories
Appendix Include additional resources or reference materials if applicable eg. list of contacts	

8. Communication Networks

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol establishes standardized procedures, guidelines, and measures to safeguard maritime communication networks from cyber threats. These networks are essential for operational safety, navigation, and coordination between vessels and shore-based infrastructure. Ensuring their protection from unauthorized access, malware infections, jamming, and data manipulation is critical for maintaining secure and reliable maritime communication.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all maritime communication networks, including: • Ship-to-ship and ship-to-shore communication systems • Satellite communication (SATCOM) networks • Very High Frequency (VHF) and High-Frequency (HF) radio networks • Global Maritime Distress and Safety System (GMDSS) • Onboard IT networks supporting communication systems • Networked bridge communication and navigational systems • Cyber-physical systems that rely on communication links It covers both onboard and shore-based IT infrastructure supporting maritime communication.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	• IMO Guidelines on Maritime Cyber Risk Management • ISO/IEC 27001: Information Security Management • NIST Cybersecurity Framework • International Safety Management (ISM) Code • International Convention for the Safety of Life at Sea (SOLAS)

Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Cybersecurity Officer: Monitors and responds to cyber threats affecting communication networks. • IT Administrators: Maintain security patches, monitor traffic, and prevent unauthorized access. • Bridge Officers & Crew: Observe best practices, report anomalies, and verify the integrity of communication links. • External Auditors: Conduct cybersecurity assessments of communication network vulnerabilities.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	• Regular vulnerability scans of communication network infrastructure. • Monitoring network activity for unauthorized access attempts. • Secure backups of communication logs stored on independent systems. • Redundant communication channels (e.g., VHF, SATCOM, HF) to ensure failover capability.
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** • Implement Role-Based Access Control (RBAC) to restrict access to communication networks. • Require Multi-Factor Authentication (MFA) for remote access to communication servers. • Use strong password policies with periodic mandatory updates.
	Data Protection • Encrypt data transmissions between ship and shore-based stations. • Use digital signatures to verify the authenticity of critical communication data. • Implement end-to-end encryption for sensitive messages and emergency communications. • Employ secure voice communication protocols for sensitive maritime operations.
	System Security • Apply timely security patches and software updates.

	• Monitor systems for anomalies, such as unauthorized configuration changes. • Verify the integrity of communication logs to detect potential cyber threats. • Implement redundant power supplies and failover mechanisms for critical communication systems.
	Network Security • Deploy firewalls and Intrusion Detection Systems (IDS) to monitor traffic for anomalies. • Segregate communication networks from other onboard IT systems to reduce risk exposure. • Analyze system logs for unauthorized modifications to communication protocols. • Implement frequency hopping and anti-jamming technologies to mitigate radio interference threats. • Utilize network segmentation to limit the impact of potential cyber incidents.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** • Monitor for unusual data transmissions or signal jamming. • Cross-check critical messages with alternative communication methods. • Identify and respond to denial-of-service (DoS) attacks on communication networks.
	Incident Reporting • Immediate reporting of cybersecurity incidents to the Cybersecurity Officer. • Document and categorize incidents based on severity and potential impact.
	Incident Containment • Isolate affected networks to prevent further data breaches. • Switch to backup communication channels (e.g., VHF or HF radio) in case of primary system compromise. • Conduct real-time traffic analysis to identify ongoing threats.

	Post-Incident Recovery • Restore data from backups after validating integrity. • Investigate root causes to prevent future incidents. • Update security protocols based on lessons learned. • Ensure resilience testing is conducted post-recovery.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Simulation-Based Training: Conduct regular exercises simulating cyberattacks on communication networks. • Ongoing Security Education: Keep personnel updated on emerging cybersecurity threats and defensive tactics.
	Cybersecurity Drills • Train crew to identify and respond to cyber threats affecting communication networks. • Build awareness of social engineering tactics used to manipulate maritime communications. • Conduct tabletop exercises to simulate emergency communication failures.
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Conduct internal and external audits to assess the effectiveness of cybersecurity measures. • Review network logs for signs of cyber threats or unauthorized access. • Ensure compliance with international cybersecurity standards. • Implement continuous monitoring solutions for real-time network security assessment.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Maintain secure communication between onboard and shore-based personnel. • Establish secure communication channels for reporting and responding to cybersecurity incidents. • Define emergency communication protocols in case of total network failure.
Review and Update Cycle	• Biannual reviews of cybersecurity protocols for maritime communication networks.

Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Immediate updates in response to significant cybersecurity incidents or emerging threats. • Quarterly vulnerability assessments to ensure evolving threats are addressed.
Appendix Include additional resources or reference materials if applicable eg. list of contacts	• List of emergency communication contacts. • Reference materials on best cybersecurity practices for maritime communication. • Best practices for network hardening and secure configuration guidelines

9. Onboard Entertainment Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol aims to establish standardized procedures, guidelines, and measures to safeguard digital assets, systems, and operations from cyber threats, including SQL injection, phishing, Denial of services (DoS), and man in the middle (MITM) attacks. The protocol ensures resilience against these evolving cyber threats.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all digital systems, databases, networks, and operational platforms like **onboard entertainment systems** that are susceptible to SQL injection, phishing attempts, denial of service attacks, and MITM interceptions.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	This protocol adheres to the following standards and regulations: IMO Guidelines on Maritime Cyber Risk Management
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	• Cybersecurity Officer: Oversees system monitoring and response to SQL injection, phishing, DoS, and MITM attacks. • IT Administrators: Ensure regular security updates, including protection against SQL injection vulnerabilities in databases, DoS mitigation tools, and network encryption for MITM attack prevention. • Employees and Crew Members: Follow best practices to avoid phishing attempts and report any suspicious activities. • External Auditors: Perform cybersecurity assessments focusing on vulnerabilities related to SQL injection, DoS attacks, and encryption standards for MITM.
Risk Assessment and Threat Identification	• Systematic Scanning: Utilize advanced scanning software to regularly assess digital

Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	systems, networks, and applications for vulnerabilities that could be exploited by cyber threats. This includes scanning for both known vulnerabilities and unusual system behaviors that might indicate emerging threats. • External Audits: Engage with third-party cybersecurity experts to conduct external audits of the maritime operations' cybersecurity practices. These audits provide an objective review of the current security measures and identify potential areas for improvement.
Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** • Role-Based Access Control (RBAC): Implement RBAC to ensure that access to systems is based on the user's role within the organization, limiting the exposure of sensitive systems and data. • Multi-Factor Authentication (MFA): Enforce MFA for all critical systems to significantly reduce the risk of unauthorized access.
	Data Protection • Parameterized Queries: Utilize parameterized queries for all database interactions to eliminate the risk of SQL injection. • Data Encryption: Encrypt sensitive data both at rest and in transit to secure information from unauthorized interception and access.
	System Security • Regularly patch systems to close vulnerabilities that could lead to SQL injection or DoS attacks. • Secure web applications by regularly testing against SQL injection using penetration testing. • Deploy email filtering systems to detect phishing emails.

	• Educate employees on identifying phishing attempts and enforce strict policies regarding email attachments and links.
	Network Security • End-to-End Encryption: Apply strong encryption protocols to all data transmissions to protect data integrity and confidentiality against interception. • Intrusion Detection Systems (IDS): Use IDS to monitor for signs of an impending or ongoing attack, especially for high volumes of traffic that could indicate a DoS attack.
Incident Response Plan Outline the steps to be taken in case of a cyber incident, detailing how to respond, contain, and recover from an attack.	**Incident Detection** • Use monitoring tools to detect anomalies such as large amounts of traffic (indicating DoS), unauthorized access attempts (MITM), or abnormal database queries (SQL injection). • Rapid Response Teams: Designate and train rapid response teams for different types of cyber incidents to ensure quick and effective handling of potential breaches.
	Incident Reporting • Automated Alerting Systems: Utilize automated systems to ensure that any anomalous activity is immediately reported to the cybersecurity team for rapid assessment.
	Incident Containment • System Isolation and Quarantine: Quickly isolate and quarantine affected systems or network segments. This includes disconnecting databases and systems from the network, ensuring that the threat does not spread and minimizing the impact on unaffected areas. • Traffic Control and Filtering: Use firewalls and intrusion prevention systems to control, filter, and reroute network traffic to and from compromised systems. This helps prevent the escalation of the incident and protects

	critical network infrastructure from further exposure. • Access Control Adjustments: Temporarily tighten access controls and disable or modify user accounts that are suspected of being compromised. This step is crucial to securing the network against unauthorized access and preventing further exploitation of system vulnerabilities. • Secure Communication Channels: Re-establish and secure communication channels to ensure that response teams can coordinate effectively without risking further exposure. Replace any compromised security certificates to maintain the integrity of data transmissions. • Backup Activation and System Restoration: Activate standby systems or revert to secure backups to maintain operational continuity. This ensures that essential functions remain online while primary systems are being cleansed and restored.
	Post-Incident Recovery • System Recovery and Validation: Prioritize the restoration of affected systems by ensuring that they are thoroughly cleaned and restored to their original state. Validate the integrity and functionality of the systems before bringing them back online to ensure they are free from any threats. • Data Restoration: Carefully restore data from backups after verifying that the backups are free of any malicious alterations. Implement strict validation processes to ensure that all restored data maintains its integrity and confidentiality. • Root Cause Analysis: Conduct a comprehensive root cause analysis to determine the specific vulnerabilities that were exploited and the origin of the incident.

	• Security Enhancements: Based on the findings from the root cause analysis, implement necessary updates and enhancements to cybersecurity measures to prevent similar incidents. • Document all aspects of the incident response and recovery process for future reference and for compliance purposes. • Review and Training: Review the incident with key personnel and update training materials based on lessons learned. Conduct training sessions to ensure all relevant staff are aware of the new security measures and understand their roles in preventing future incidents.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** • Simulation-Based Training: Regularly conduct realistic simulation exercises to prepare staff for actual attack scenarios, emphasizing the importance of security practices and procedures. • Ongoing Security Education: Offer continuous education on emerging cybersecurity threats and defensive tactics to keep personnel updated and prepared.
	Cybersecurity Drills • Regularly Scheduled Drills: Conduct drills at regular intervals to test the effectiveness of both the technical and procedural aspects of the cybersecurity protocols. • Scenario-Based Training: Design and implement a variety of attack scenarios to challenge the readiness of the cybersecurity team and other relevant personnel. Scenarios should cover a wide range of potential threats, from data breaches to system intrusions and phishing attacks.
Audit and Compliance Monitoring Specify how compliance with the cybersecurity protocols	• Conduct both internal and external audits focusing on the detection and mitigation of SQL injection, DoS, MITM, and phishing risks.

will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	• Review system logs for signs of potential attacks, ensuring protocols are in place and functioning effectively.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	• Maintain a clear line of communication between onboard and shore-based personnel, especially in the event of phishing, DoS, or MITM attacks to ensure timely response and containment. • Secure communication channels must be in place to prevent interception by MITM attacks.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	• Conduct formal reviews of the cybersecurity protocols every six months to ensure they are up-to-date and effective against current cyber threats. • In addition to scheduled reviews, the protocols must be promptly reviewed and potentially updated in response to significant new cybersecurity incidents or news related to exploits affecting software and systems used within maritime operations.
Appendix Include additional resources or reference materials if applicable eg. list of contacts	

10. Cargo Management Systems

Maritime Cybersecurity Protocol	
Purpose Provide a clear purpose of the protocol. This section explains the intent of the document, which is to establish procedures, standards, and guidelines to ensure the cybersecurity of maritime assets and operations.	This protocol establishes standardized procedures, guidelines, and security measures to protect Cargo Management Systems (CMS) from cyber threats. As CMS plays a crucial role in cargo tracking, planning, loading, and unloading, its security is essential for ensuring efficient and uninterrupted maritime logistics. The protocol aims to safeguard CMS against unauthorized access, data breaches, malware infections, ransomware, and manipulation of cargo-related data. By securing these systems, the protocol helps maintain the integrity, confidentiality, and availability of cargo operations, preventing disruptions that could impact vessel safety, port efficiency, and the global supply chain.
Scope Define the scope of the cybersecurity protocol, detailing the specific assets, systems, and operations it covers.	This protocol applies to all digital assets, networks, and operational components related to Cargo Management Systems (CMS) onboard ships and in shore-based facilities. It covers cybersecurity measures for: - Cargo planning and loading software used for stowage optimization and weight distribution. - Cargo tracking and monitoring systems, including RFID, IoT sensors, and real-time data feeds. - Database and network infrastructure storing and transmitting cargo manifests, schedules, and logistics data.
Applicable Standards and Regulations Example: IMO Guidelines on Maritime Cyber Risk Management	- IMO Guidelines on Maritime Cyber Risk Management - ISO/IEC 27001: Information Security Management - NIST Cybersecurity Framework - International Safety Management (ISM) Code
Roles and Responsibilities Define the roles and responsibilities of various stakeholders involved in cybersecurity management.	- Cybersecurity Officer: Oversees the security of Cargo Management Systems (CMS), manages incident response, and ensures compliance with cybersecurity policies. - IT Administrators: Implement security updates, monitor network traffic, and maintain access controls

	to protect CMS from cyber threats. - Cargo Operations Officers: Ensure secure handling of cargo data, verify the integrity of digital cargo manifests, and report suspicious system behavior. - Ship and Shore-based Personnel: Follow cybersecurity best practices, use authorized access credentials, and report anomalies in CMS operations. - External Security Auditors: Conduct periodic cybersecurity assessments, penetration testing, and compliance checks to identify vulnerabilities in CMS infrastructure.
Risk Assessment and Threat Identification Provide a risk management framework that identifies and assesses risks associated with cyber threats. Include methodologies for assessing vulnerabilities and how to prioritize risks based on impact and likelihood.	- Regular Vulnerability Scans: Conduct routine security assessments on Cargo Management Systems (CMS) software, databases, and network infrastructure to identify exploitable weaknesses. - Continuous Network Monitoring: Utilize intrusion detection systems (IDS) and security information and event management (SIEM) tools to detect unauthorized access attempts and anomalies in CMS operations. - Data Encryption: Implement end-to-end encryption for cargo-related data transmissions to prevent unauthorized interception and manipulation. - Access Control Mechanisms: Enforce role-based access control (RBAC) and multi-factor authentication (MFA) to limit system access to authorized personnel only. - Incident Response Planning: Establish predefined protocols for detecting, reporting, and mitigating cyber incidents affecting CMS. - Redundant Data Storage and Backup: Maintain secure, regularly updated backups of cargo data to ensure business continuity in case of cyberattacks or system failures. - Third-Party Security Audits: Engage external cybersecurity specialists to perform penetration testing and compliance evaluations on CMS infrastructure.

Cybersecurity Controls and Measures Describe the specific cybersecurity measures to be implemented.	**Access Control** - Role-Based Access Control (RBAC): Restrict access to Cargo Management Systems (CMS) based on user roles, ensuring that only authorized personnel can modify cargo data. - Multi-Factor Authentication (MFA): Require MFA for all critical CMS access points, especially for remote logins and administrative privileges.
	Data Protection - Data Encryption: Encrypt cargo manifests, tracking data, and communication logs both in transit and at rest using AES-256 encryption. - Digital Signatures: Implement digital signatures to verify the authenticity and integrity of cargo-related documents and transactions. - Secure API Gateways: Ensure that third-party integrations, such as port and customs systems, use secure authentication and encrypted data exchanges.
	System Security -Regular Patching and Updates: Apply timely security patches to CMS software and underlying infrastructure to mitigate vulnerabilities. - Anomaly Detection: Deploy machine learning-based monitoring to detect irregular modifications in cargo data that could indicate cyber manipulation. - Access Logging and Auditing: Maintain detailed logs of all system access and data modifications, with regular audits to identify suspicious activity.
	Network Security - Firewalls and Intrusion Detection Systems (IDS): Implement firewalls to filter unauthorized traffic and IDS to monitor for potential cyberattacks. - Network Segmentation: Isolate CMS from general onboard IT systems to minimize the impact of breaches in other shipboard networks. - Secure Remote Access: Restrict remote access to CMS through Virtual Private Networks (VPNs) with strict access control policies.
Incident Response Plan Outline the steps to be taken in case of a cyber incident,	**Incident Detection** - Cargo Data Anomaly Monitoring: Use real-time monitoring tools to detect unauthorized modifications

detailing how to respond, contain, and recover from an attack.	to cargo manifests, unexpected system access, or irregular data transmissions. - Network Traffic Analysis: Identify abnormal traffic patterns that may indicate a cyberattack, such as Distributed Denial-of-Service (DDoS) attempts or unauthorized API calls. - Access Log Audits: Continuously review access logs to detect unauthorized login attempts, privilege escalations, or credential misuse.
	Incident Reporting - Immediate Escalation: Promptly notify the Cybersecurity Officer and IT Administrators of any detected threats. - Incident Categorization: Classify incidents based on severity, from minor unauthorized access attempts to full-scale data breaches, ensuring an appropriate response level. - Automated Alerts: Implement automated alerting systems to notify relevant personnel of detected cybersecurity anomalies in Cargo Management Systems (CMS).
	Incident Containment - System Isolation: Quarantine affected CMS components to prevent the spread of malware or data corruption. - Account Suspension: Immediately disable or revoke access for compromised user accounts. - Traffic Filtering and Blocking: Use firewalls and intrusion prevention systems (IPS) to block malicious IP addresses and unauthorized network traffic. - Backup Activation: Switch to standby CMS backups to ensure operational continuity while the affected systems are being secured.
	Post-Incident Recovery - System Restoration and Validation: Reload CMS configurations from verified, uncompromised backups, ensuring the integrity of cargo-related data. - Root Cause Analysis: Conduct a forensic investigation to identify vulnerabilities that were exploited and the origin of the attack. - Security Enhancements: Implement additional

	cybersecurity measures, such as stricter access controls or enhanced encryption, based on the findings. - Documentation and Training: Maintain detailed records of the incident response process, update security protocols, and conduct staff training to prevent similar incidents in the future.
Cybersecurity Training and Awareness Provide guidelines for conducting regular training and awareness programs for all personnel involved in maritime operations, including crew members and shore-based staff.	**Training Programs** - Simulation-Based Training: Conduct regular cyberattack simulations focused on threats to Cargo Management Systems (CMS), such as ransomware targeting cargo data, unauthorized manifest modifications, and API-based attacks on logistics platforms. - Ongoing Security Education: Provide continuous training for crew members and shore-based personnel on emerging cyber threats, including phishing, insider threats, and malware targeting CMS infrastructure. - Cargo Data Integrity Workshops: Educate personnel on secure handling, transmission, and validation of cargo-related information to prevent unauthorized modifications or data breaches.
	Cybersecurity Drills - Scenario-Based Drills: Implement drills that simulate cyber incidents affecting CMS, such as data tampering in cargo manifests, GPS interference affecting cargo tracking, or unauthorized API access to cargo booking systems. - Pre-Voyage Cybersecurity Briefings: Before each voyage, conduct briefings on cybersecurity best practices, incident response protocols, and data validation techniques to ensure cargo integrity. - Awareness on Social Engineering Attacks: Train staff on recognizing and mitigating social engineering tactics, such as fraudulent cargo clearance requests or phishing emails designed to compromise CMS credentials.
Audit and Compliance Monitoring Specify how compliance with	- Internal and External Audits: Conduct regular audits to assess the security of Cargo Management Systems (CMS), focusing on unauthorized access, data

the cybersecurity protocols will be monitored and audited. Include both internal and external audits and the frequency of such reviews.	manipulation, ransomware threats, and API security vulnerabilities. - Log Review Protocols: Continuously analyze system logs, cargo data transactions, and access records for signs of potential cyber threats or anomalies. - CMS-Specific Audits: Perform quarterly internal audits covering database integrity, cargo tracking security, and compliance with access control policies. - Annual External Review: Engage cybersecurity specialists to conduct an in-depth assessment of CMS cybersecurity measures, evaluating compliance with maritime cybersecurity standards and identifying potential vulnerabilities.
Communication and Coordination Provide a clear communication strategy during both normal operations and in case of a cybersecurity event.	- Onboard and Shore-Based Coordination: Ensure continuous communication between vessel crew and shore-based cybersecurity teams for real-time monitoring of Cargo Management Systems (CMS) security. - Secure Incident Reporting: Implement an encrypted reporting system for crew and personnel to report cybersecurity incidents immediately, ensuring rapid assessment and mitigation. - End-to-End Encryption: Apply AES-256 or TLS 1.3 encryption to all CMS-related communications to prevent interception or tampering. - Controlled Network Access: Segregate operational CMS communications from public or unsecured networks to reduce exposure to cyber threats. - Regulatory and Industry Coordination: Establish predefined communication protocols with maritime cybersecurity authorities (IMO, port authorities, and national cybersecurity agencies) to ensure compliance and effective response to large-scale cyber incidents.
Review and Update Cycle Define how often the protocols will be reviewed and updated to ensure they remain relevant and effective against emerging threats.	- Biannual Cybersecurity Reviews: Conduct comprehensive reviews of Cargo Management System (CMS) cybersecurity protocols every six months to assess effectiveness against emerging threats. - Regulatory and Compliance Updates: Align

	cybersecurity protocols with the latest IMO, NIST, and ENISA guidelines, ensuring adherence to evolving maritime cybersecurity regulations. - Technology and Threat Landscape Assessment: Regularly evaluate advancements in encryption standards, intrusion detection systems (IDS), and AI-driven threat mitigation techniques to enhance CMS security. - Immediate Protocol Updates: Revise cybersecurity measures promptly in response to newly discovered vulnerabilities, cyber incidents, or security advisories affecting maritime CMS infrastructure.
Appendix Include additional resources or reference materials if applicable eg. list of contacts	