

Cyber Risk Management Policy



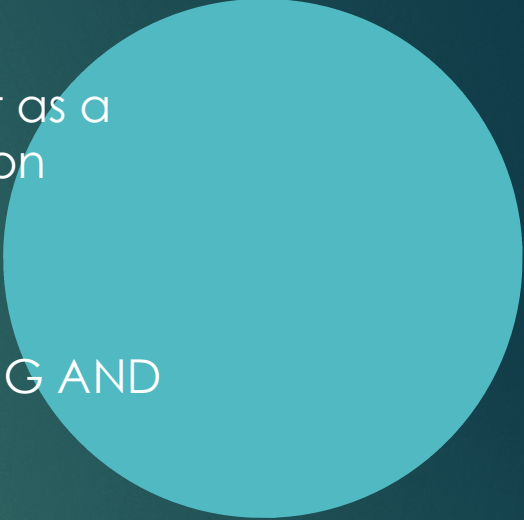
Objective

- ▶ To support, safe and secure, and resilient operation of essential IT/OT Systems by implementing measures to protect against operational, safety or security failures as a consequence of information or systems being intentionally or unintentionally corrupted, hacked, lost or compromised

Scope

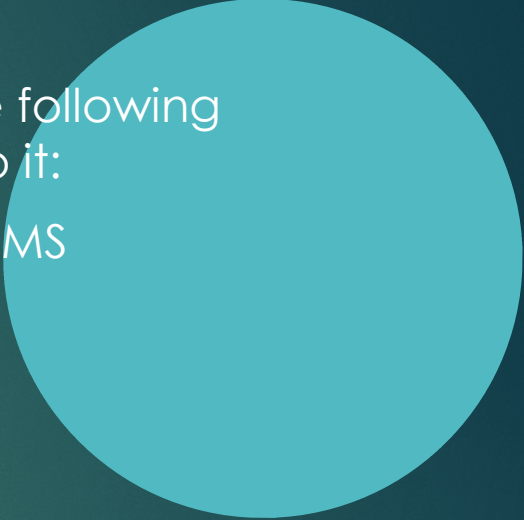


This should be considered as best practice for all systems but as a minimum must apply Operational technology and Information technology related to the following functions:

- ▶ BRIDGE and SAFETY CENTER SYSTEM
 - ▶ MACHINERY AUTOMATION, POWER MANAGEMENT, STEERING AND PROPULSION CONTROL SYSTEM
 - ▶ REMOTE COMMUNICATION / ACCESS SYSTEMS
- 


Scope



- ▶ Whilst not mandatory at this stage systems related to the following functions should be prioritized for full inclusion into it:
 - ▶ PASSENGER SERVICING AND MANAGEMENT SYSTEMS
 - ▶ PASSENGER FACING PUBLIC NETWORKS
 - ▶ ADMINISTRATIVE AND CREW WELFARE SYSTEMS
- 

Philosophy



- ▶ All of this is based on MSC-FAL1 Circ.3 Guidelines on Maritime Cyber Risk Management
 - ▶ Cyber Risk Management is a continuous process of development, monitoring and improvement
- 

Philosophy



- ▶ The process is divided into five main elements:
- ▶ Identify the relevant measures before cyber incidents occur including conducting cyber risk assessments
- ▶ Protect the systems by developing and implementing safeguards including awareness training, access control and network segmentation
- ▶ Detect possible cyber incidents by developing and implementing appropriate activities including implementing continuous monitoring processes

Philosophy



- ▶ Respond to detected cyber incidents is an appropriate way including response plan and mitigating actions
 - ▶ Recover services disturbed by cyber incidents including a recovery plan
- 

Process: IDENTIFY

- ▶ The head of Cyber Risk management must ensure that cyber risk are identified and assessed using the following:
- ▶ A register is developed and maintained of essential IT/OT systems including hardware, data flow, software
- ▶ Each essential IT/OT system is assigned a responsible Owner and that system owner and responsibilities are clearly defined
- ▶ A cyber risk assessment is undertaken and maintained over time and that resulting risk control processes, measures and contingency plans keep risks at tolerable/acceptable levels

Process: PROTECT



- ▶ We must ensure that effective safeguards are in place to protect the following items:
- ▶ Systems are configured for their specific needs and, where appropriate, only used for their designated purposes
- ▶ Effective cyber risk management and security awareness training programs are in place
- ▶ Systems are protected by appropriate physical security measures
- ▶ Networks are appropriately segmented to limit any undesirable interactions between systems, personnel and outside threat vectors


Process :PROTECT

- ▶ Cyber resilience requirements are defined and applied during procurement and newbuild and wherever practical, suppliers are contractually required to design-in cyber resilience and ensure long term support
- ▶ Access rights and permissions for shoreside ,shipboard and remote systems are appropriately controlled,checked,including password length ,complexity and expiry
- ▶ Remote access is limited to authorized trained personnel and ,where practical,individually authorized on each occasionn remote access interventions are made

Process :PROTECT

- ▶ Systems have appropriate anti-malware software installed and running and that virus definitions are regularly updated
- ▶ Security patches are regularly assessed, verified and implemented
- ▶ Strong processes are in place to ensure that removable devices are only used where necessary and are free from malware before usage

Protect: DETECT



- ▶ We must ensure that methods ,tools and process are always implemented to detect cyber incidents in a timely manner ,with attention concentrated on the loss f system integrity,conficentiality,availability
- ▶ Detection scope must cover all essential systems
- ▶ Cyber risk management and security awareness training programs include requirements for all system users to promptly report any abnormal event or security concern
- ▶ Procedures are in place to ensure detected cyber incidents are recorded,managed, investigated and that resultant corrective actions are implemented in a timely manner

Respond and recover



- ▶ We must ensure that:
- ▶ Cyber incident response and recovery plans which prioritize restoration of essential services, operations and capabilities in a timely manner are developed and maintained. these plans must be aligned with the Company Emergency response plan
- ▶ Training programs for cyber incident response and recovery are developed, implemented and maintained
- ▶ Cyber incident drill programs are implemented to regularly test the cyber incident response and recovery plan

Thank u!!!!!!

