****

**Internal Audit**

**ISM**

**Cyber Security Internal Audit**

|  |  |
| --- | --- |
| **Audit Date(s)** |  |

|  |  |
| --- | --- |
| **Auditor(s)** |  |
|  |

|  |  |
| --- | --- |
| **Vessel** |  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | No | Remarks |
| **Policy** |  |  |  |
| Documentation to verify Cyber Security Policy. |  |  |  |
| Person In charge (PIC) |  |  |  |
| Do the crew know the identity of the Cyber Security Officer (CSO)? |  |  |  |
| Do the crew know the CSO’s Role? |  |  |  |
| **Asset Management** |  |  |  |
| Have users been provided with a Password. |  |  |  |
| Have Password been changed after the first login and password principles compliant. |  |  |  |
| Are Computer and Devices free of written passwords and login in the proximity |  |  |  |
| Are incidents reported to the Ship Cyber Security Officer. |  |  |  |
| Are all terminal logged of when not in use. |  |  |  |
| Are restrictions in place for unauthorised visitors to access IT facilities onboard |  |  |  |
| **Antivirus** |  |  |  |
| Is a company approved Antivirus installed onboard on all computers. |  |  |  |
| Is the antivirus enable and is scanning. |  |  |  |
| Are there any obsolete operating system and software installed. |  |  |  |
| **Network** |  |  |  |
| Are authorized crew users of the vessel non business network |  |  |  |
| Are crew trained and knowledgeable on activities deemed unproductive by the company not to be undergone on company’s network (harassing, obscene/offensive/improper material, hacking etc) |  |  |  |
| Are there currently Security protection on wireless networks |  |  |  |
| **Information Security** |  |  |  |
| Are Users crew aware of procedures referring tosensitive data request from suspicious requests of third parties. |  |  |  |
| **Removable Media** |  |  |  |
| Is only company USB used on vessels computers |  |  |  |
| Are dedicated USB used only for the ECDIS and properly labelled. |  |  |  |
| **Back Up** |  |  |  |
| Is back up of data carried out on vessels computers. |  |  |  |
| **Risk Assessment** |  |  |  |
| Are any cyber security risk identified by the vessels, reported to the Company Cyber Security Officer. |  |  |  |
| Have risk Assessments been shared with the vessels from the office? |  |  |  |
| **Training** |  |  |  |
| Have crew received training in cyber security and are familiar with company procedures and policy. |  |  |  |

|  |
| --- |
| **Auditor(s)** |
| Ian McIntosh-Oakley | ---------- |