IT 03 – Cyber Security Checklist

1. Has a cyber risk assessment review been completed recently (last 6 months)? Yes ⬜
2. Is access to communications cabinets/rooms secure? Yes ⬜
3. Are changes to systems properly tracked and formalized?...................................................Yes ⬜
4. Has the business network been checked to ensure no unauthorised equipment is connected? Yes ⬜
5. Are USB port locks in use for critical systems? Yes ⬜
6. Is Malware protection in place for critical systems?..............................................................Yes ⬜
7. Have all computers been checked to ensure no warning messages displayed on screens (virus etc) Checked ⬜
8. Are cell phone batteries being charged via USB ports? Checked ⬜
9. Is the incident management process implemented? Yes ⬜
10. Is cyber safety awareness actively promoted? Yes ⬜
11. Ensure passwords meet company criteria and are not on display Checked ⬜
12. Is there a process for backing up important documents and data? Yes ⬜
13. Are master disks stored in a safe place? Yes ⬜
14. Have the computer systems been replaced in the last 4 years? Yes ⬜
15. Is the functional account owner properly appointed?.......................................................... Yes ⬜
16. Is the third party software monitored from Silversea?..........................................................Yes ⬜

**Note:** If the answer is “No” to any of these checks, make the necessary changes to meet the cyber safety requirements.

Guidance Notes

**Note:** The numbers/titles noted below in brackets are the sections of the Vessel Management System which will offer additional guidance.

1. The Cyber Risk Assessment is required to be completed and returned to Master periodically for review. **(3.6 Risk Evaluation)**
2. To prevent unauthorized access, damage, interference to information system assets and interruption to business activities, controls and safeguards must be implemented. **(4.7 Physical and Environmental Security)**
3. VMS Change Management procedure will be followed for any major electronic equipment changed or software upgrades **(4.6 Information systems Acquisition, Development and Maintenance)**
4. No unauthorized equipment is to be connected to network. WiFi access points must not be connected to vessel business network. **(4.5 Communication and Operation Management)**
5. USB ports for critical systems must be physically protected. Authorized access will be logged. **(4.5 Communication and Operation Management)**
6. To avoid cyber attacks from malwares and viruses, Antivirus, Firewall and awareness and training programs must be performed. **(4.5 Communication and Operation Management)**
7. Anti-virus or system alerts will be noted and investigated. On seeing any alerts, IT Team will be contacted and made aware. **(4.4 Information Security Incident Management)**
8. Personal devices should not be connected to vessel business network **(4.5 Communication and Operation Management)**
9. The VMS provides guidelines on actions against incidents. **(4.4 Information Security Incident Management)**
10. All crew should have competed Cyber Safety training course. Materials such as posters and notices will be prominently displayed. **(3.7 Training & Awareness)**
11. Passwords will not be written and made available for viewing. Only the vessel support accounts will provide administrative level access to computer systems. **(4.1 Access Control)**
12. Important electronic documents and data will be stored in an area that is regularly backed up in the event of loss. **(4.5 Communication and Operation Management)**
13. The Master disks to the media which contains the ship board software should be kept and stored safely in a safe place. **(4.6 Information systems Acquisition, Development and Maintenance)**
14. To maintain full product support and system updates compatibility, system are to be replaced on an average of 4 years. **(3.2 Standing Instructions)**
15. The owner of the functional account must be properly tracked. **(4.1 Access Control)**
16. Every third party must be registered and softwares must be monitored. **(4.3 Third Party Management)**