IT 03 – Cyber Security Checklist

1. Has a cyber risk assessment review been completed in the last 6 months? Yes ⬜
2. Has a change form been submitted for any new or updated electronic equipment? Yes ⬜
3. Is access to communications cabinets/rooms secure? Yes ⬜
4. Has the business network been checked to ensure no unauthorised equipment is connected? Yes ⬜
5. Are USB port locks in use? Yes ⬜
6. Have all computers been checked to ensure no warning messages displayed on screens (virus etc) Checked ⬜
7. Are cell phone batteries being charged via USB ports? Checked ⬜
8. Is there a cyber response plan available onboard? Yes ⬜
9. Is cyber safety awareness actively promoted onboard? Yes ⬜
10. Ensure passwords meet company criteria and are not on display Checked ⬜
11. Is there a process for backing up important documents and data? Yes ⬜
12. Are software disks stored in the Masters safe? Yes ⬜
13. Are PC’s locked automatically after a set period of time 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 ( ) are the sections of the V.Group Cyber Security Plan which will offer additional guidance.

1. The Cyber Risk Assessment tool is required to be completed and returned to VST every 6 months for review. **(2.2 System Audit and Risk Assessment)**
2. VMS Change Management procedure will be followed for any major electronic equipment changed or software upgrades **(2.3 Change Management)**
3. Physical access to sensitive communications equipment areas will be controlled. Equipment rooms will be locked or monitored, communications cabinets will be closed and locked. **(2.6.1 Access Controls – Physical)**
4. No unauthorised equipment is to be connected to network. WiFi access points must not be connected to vessel business network. **(2.4 Communications Networks)**
5. USB ports will be physically protected. Authorised access will be logged. **(2.6.1 Access Controls – Physical)**
6. Anti-virus or system alerts will be noted and investigated. On seeing any alerts, VST will be contacted and made aware.
7. Personal devices will not be connected to vessel business network
8. The V.Ships Cyper Security Plan is contained within the SSP as addeddum. The CSP contains security incident process
9. All crew should have competed V.Ships seafarers Cyber Safety training course. Materials such as posters and notices will be prominently displayed.
10. Passwords will not be written and made available for viewing. Only the vessel support accounts will provide administrative level access to computer systems. **(2.6.2 Access Controls – Network/Application)**
11. Important electronic documents and data will be stored in an area that is regularly backed up in the event of loss. **(2.8.2 Data Backups – Data Files)**
12. The Master disks to the media which contains the ship board software should be kept and stored safely in the Masters safe. **(2.1 Standing Orders)**
13. PC’s should not lie unlocked when not in use. **(2.6.2 access Controls – Network/Application)**