



ST. VINCENT AND THE GRENADINES

MARITIME ADMINISTRATION

CIRCULAR N° SOL 079

GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD COMPUTER-BASED NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

MSC.1/Circ.1704

TO: **SHIPOWNERS, SHIP MANAGERS, MASTERS,
RECOGNIZED ORGANIZATIONS, SHIPBUILDERS AND
MANUFACTURERS**

APPLICABLE TO: All ships fitted with shipboard computer-based navigation and communication equipment and systems.

EFFECTIVE FROM: Date of this Circular

Date: 27 July 2026

1. General

1.1 This Circular provides guidance on the software maintenance of shipboard computer-based navigation and communication equipment and systems in accordance with IMO MSC.1/Circ.1704, *Guidelines for Software Maintenance of Shipboard Computer-Based Navigation and Communication Equipment and Systems*.

1.2 The purpose of this Circular is to promote the safe, secure and controlled maintenance of software installed on navigation and communication equipment throughout its operational life.

1.3 Companies should establish procedures within their Safety Management System (SMS) for the planning, authorization, execution and documentation of software maintenance affecting navigation and communication equipment.

1.4 Software maintenance should be carried out in accordance with the equipment manufacturer's instructions and should ensure that the equipment continues to comply with its type approval and any applicable class and statutory requirements.

1.5 Software maintenance should ensure that:

1. operational safety is maintained;
2. cybersecurity risks are appropriately managed;
3. software integrity is preserved;
4. software versions remain traceable; and

5. the vessel can be restored to a safe operational condition should a software update fail.

2. Company Responsibilities

Companies should ensure that procedures include, as appropriate:

1. maintenance of an inventory of installed software and software versions;
2. assessment and approval of proposed software updates;
3. planning of software maintenance so as not to compromise the safety of navigation;
4. verification that updates originate from authorized sources;
5. backup of existing software, configuration data and settings before installation;
6. testing following software installation;
7. restoration procedures in the event that software installation is unsuccessful;
8. maintenance of records of software updates and maintenance activities;
9. appropriate cybersecurity precautions during software maintenance;
10. control of remote software maintenance, including authorisation, access control and recordkeeping where such maintenance is performed.

3. Service Providers

3.1 Software maintenance should be carried out by manufacturers or service providers authorized by the equipment manufacturer.

3.2 Personnel performing software maintenance should be appropriately trained and competent for the equipment concerned.

3.3 Upon completion of software maintenance, the service provider should provide a report identifying, as applicable:

1. equipment maintained;
2. software version installed;
3. date of installation;
4. tests performed;
5. any limitations identified; and
6. confirmation that the equipment has been tested and remains operational.

4. Shipboard Responsibilities

4.1 The Master should ensure that:

1. software maintenance is carried out in accordance with the Company's SMS;
2. operational limitations during software maintenance are adequately managed;
3. appropriate records are retained on board; and
4. defects identified following software maintenance are reported to the Company without delay.

5. Surveys

5.1 Recognized Organizations acting on behalf of this Administration should, as appropriate, verify, during ISM audits and statutory surveys that Companies have implemented procedures consistent with this Circular and IMO MSC.1/Circ.1704.

Annex to this Circular:

- MSC.1/Circ.1704 – *Guidelines for Software Maintenance of Shipboard Computer-Based Navigation and Communication Equipment and Systems.*



E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611

MSC.1/Circ.1704
6 July 2026

GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD COMPUTER-BASED NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

- 1 The Maritime Safety Committee, at its 111th session (13 to 22 May 2026), approved the *Guidelines for software maintenance of shipboard computer-based navigation and communication equipment and systems*, as set out in the annex, prepared by the Sub-Committee on Navigation, Communications and Search and Rescue (NCSR), at its twelfth session (13 to 22 May 2025).
- 2 The aim of these Guidelines is to ensure that software maintenance carried out on shipboard computer-based navigation and communication equipment and systems is conducted in accordance with a controlled and standardized process.
- 3 Member States and international organizations are invited to bring these Guidelines to the attention of shipping companies, shipboard navigation and communication equipment manufacturers, service providers, mariners and all Parties concerned.

ANNEX

GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD COMPUTER-BASED NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

1 Introduction

1.1 These Guidelines provide guidance for software maintenance of shipboard equipment and systems specified in paragraph 2.1.

1.2 The detailed procedures covered by these Guidelines are provided in sections 5 to 12.

2 Application

2.1 These Guidelines apply to shipboard computer-based equipment and systems specified or referred to in chapters IV (Radiocommunications) and V (Safety of Navigation) of the International Convention for the Safety of Life at Sea, 1974, that are capable of undergoing software maintenance.

2.2 These Guidelines apply to the methods of software maintenance defined in paragraph 3.8.

2.3 These Guidelines may be applied on a voluntary basis to any shipboard computer-based equipment and system not included under paragraph 2.1 that is capable of undergoing software maintenance, including those listed in appendix 3.

3 Definitions

3.1 *Category of software maintenance* means the type of software maintenance event based on the reason for undertaking the maintenance, which may be one or more of the following:

- .1 bug fix (resolving software errors and improving performance/stability);
- .2 feature release (adding functionality);
- .3 compliance maintenance (maintaining conformity with regulations);
- .4 security update (protecting against cyber threats); and
- .5 obsolescence maintenance (addressing software and/or hardware that is no longer supported).

3.2 *Contracted Service Provider* means the entity contracted by the Company to facilitate the planning and execution of a software maintenance event. The Contracted Service Provider may be the Manufacturer or a third-party organization

3.3 *Certified Service Technician* means the employee of the Contracted Service Provider who is trained and certified by the Manufacturer in accordance with section 5 and who executes the software maintenance event.

3.4 *Company*, for the purpose of these Guidelines, means the shipowner or any other entity or person, such as the manager or the bareboat charterer, which has assumed the responsibility for the operation of the ship from the shipowner.

3.5 *Controlled network* means a shipboard network that has been designed to operate such that it does not pose any security risks to any connected network nodes.

3.6 *Critical update* means a software maintenance event that the Manufacturer has identified as critical to restoring or maintaining proper performance of the shipboard computer-based equipment or system.

3.7 *Manufacturer* means the original manufacturer of a shipboard computer-based equipment or system, or any entity which has taken legal and legitimate responsibilities for such equipment or system when the original manufacturer no longer exists or supports the equipment or system.

3.8 *Method of software maintenance* means the method by which software maintenance is undertaken, which may be:

- .1 on board (carried out on the ship);
- .2 onshore (carried out off the ship, for example, at the premises of the Contracted Service Provider); or
- .3 remote (executed by accessing the shipboard computer-based system or equipment from a location external to the ship via communication links).

3.9 *Plan of approach* means a detailed description of the work to be undertaken in support of software maintenance, including appropriate assessments of the risks involved.

3.10 *Removable media/storage devices* means portable equipment used during software maintenance, including but not limited to USB memory sticks, laptop computers and external disk drives.

3.11 *Shipboard computer-based equipment and systems*, for the purpose of these Guidelines, means operational technology-comprising hardware and software installed or fitted on ships.

3.12 *Software* means programs and operating instructions used in shipboard computer-based equipment and systems, including firmware.

3.13 *Software maintenance* means updating, re-configuring, and associated checking of the software within shipboard computer-based equipment and systems.

3.14 *Uncontrolled equipment* means a device that is not part of a controlled network.

3.15 *Uncontrolled network* means a shipboard network that does not meet the definition of a controlled network.

4 General provisions

4.1 The Company should ensure that software maintenance of computer-based communication and navigation equipment and systems on board its ships is conducted in accordance with these Guidelines.

4.2 The Company should establish and implement health, safety and environmental (HSE) procedures covering all activities set out in these Guidelines.

4.3 All persons carrying out software maintenance should be trained and certified in accordance with the guidance in section 5. When performing such activities on board ships, they should comply with instructions and procedures established by the Company.

4.4 The Manufacturer, the Contracted Service Provider, the Certified Service Technician and the Company should ensure that all software maintenance-related training and operations are conducted in accordance with *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3, as revised), as well as the specific cybersecurity recommendations provided in these Guidelines.

4.5 Software installed in accordance with these Guidelines should not compromise the type approval of the equipment or systems concerned.

5 Guidance for training and certification of service technicians by Manufacturers

5.1 Software maintenance of shipboard computer-based equipment and systems should be carried out by service technicians trained and certified in accordance with this section.

5.2 Training in the software maintenance procedures and functions of shipboard computer-based equipment and systems should be provided by the Manufacturer to the service technician. This should include cybersecurity aspects of software maintenance, including:

- .1 security controls and their validation (e.g. firewall settings);
- .2 countermeasures (e.g. network port plugs);
- .3 integrity checking of shipboard computer-based equipment and systems including how to identify that an equipment or system has been compromised;
- .4 recovery procedures, including those for user data; and
- .5 procedure for reporting security events to the manufacturer.

5.3 Upon successful completion of the training, a certificate should be issued by the Manufacturer to the service technician, specifying:

- .1 the issuing Manufacturer;
- .2 date of issue;
- .3 date of expiry;
- .4 name of the Certified Service Technician;
- .5 name of the Contracted Service Provider;

- .6 list of shipboard computer-based equipment and systems produced by the Manufacturer which the Certified Service Technician is trained to maintain; and
- .7 method(s) of software maintenance covered for each shipboard computer-based equipment and system produced by the Manufacturer (onboard, onshore, and/or remote).

5.4 The certificate should:

- .1 have a validity of no more than five years from the date of issue;
- .2 become invalid if the Certified Service Technician changes employer; and
- .3 have its validity suspended in the event the Manufacturer becomes aware of any shortfall in performance and should only be revalidated after the issuing Manufacturer is satisfied that suitable corrective action has been taken.

5.5 The Manufacturer should keep a record of all Certified Service Technicians with valid certificates and make that information available to the relevant parties upon request.

5.6 The Contracted Service Provider should make a copy of the certificate available to the Company.

6 Reports and records

6.1 Upon completion of software maintenance, an electronic service report should be completed and signed by the Certified Service Technician, who carried out the work. The electronic service report should also be countersigned by the Company's representative. The minimum content of an electronic service report is defined in appendix 1.

6.2 The Company should ensure that an onboard software log is available on the ship listing the current and previous software maintenance events conducted on shipboard computer-based equipment and systems, in accordance with appendix 2. Each software maintenance event should be recorded in the onboard software log and linked to the associated electronic service report provided by the Certified Service Technician.

6.3 Records of software maintenance events, including electronic service reports, should be stored in the onboard software log for a minimum of five years.

6.4 The onboard software log can be incorporated into an existing inventory management system.

7 Guidance for the Manufacturer

7.1 The Manufacturer should have a quality assurance system for software lifecycle activities, which documents relevant procedures, responsibilities and configuration management, including deliveries from suppliers, taking into account cyber risk management and cyber threats in connection with software maintenance.

7.2 Arrangements for software maintenance of shipboard computer-based equipment and systems should be specified in the maintenance manuals, containing detailed technical information and instructions intended for service personnel. Timely access to maintenance

manuals and any other relevant technical documentation should be provided to Contracted Service Providers and/or Certified Service Technicians.

7.3 User manuals should specify how the user can report a software error or system malfunction.

7.4 Shipboard computer-based equipment and systems should:

- .1 provide the means to display, at least on demand, the current software version or, where there is no display, provide version information by alternative means such as labelling or a standardized external interface;
- .2 allow access for maintenance purposes;
- .3 provide protection against unauthorized access¹;
- .4 where applicable², support rollback procedures which may be implemented by a full back-up of software, configuration parameters and data stored by the user; and
- .5 where applicable², include a mechanism, described in the maintenance manual along with the method of execution, to generate an on-the-spot diagnostic report after software maintenance has been performed. This mechanism should identify the software version running on the shipboard computer-based equipment and system and provide a means to check that interfaces and functionality are operating as intended after the software maintenance or a rollback has been completed.

7.5 Where shipboard computer-based equipment and systems do not support rollback procedures, the Manufacturer should make replacement equipment or systems, as appropriate, available to the Certified Service Technician.

7.6 Timely access to information pertaining to the availability of new software versions for shipboard computer-based equipment and systems should be provided to Contracted Service Providers and/or Certified Service Technicians, together with:

- .1 the category of software maintenance;
- .2 the supported method of software maintenance;
- .3 where applicable, any compatibility requirements for the hardware platform;
- .4 instructions on how to confirm the software maintenance has been successfully applied;
- .5 a description of changes as specified in paragraph 7.9; and
- .6 where applicable, updated manuals as specified in paragraph 7.9.

¹ IEC 60945 imposes limitations on access to shipboard equipment by the end user.

² The phrase "where applicable" is included as there are types of shipboard computer-based equipment and systems that cannot feasibly support this requirement.

7.7 If the Manufacturer has identified the need for software maintenance on a specific shipboard computer-based equipment or system, this information should be made available to the Contracted Service Provider and the Company, as necessary. The information should include affected software versions and guidance on how the user may check to determine if the installed software version is affected. Means for updating should be made available. If the Manufacturer does not know where the equipment or system is installed, and is therefore unable to relay the information to the Contracted Service Provider or the Company, the Manufacturer should relay the information to the known purchaser of the equipment or system concerned.

7.8 If the software maintenance is designated as a critical update by the Manufacturer, this information should be accompanied by a recommendation that the software maintenance should be performed as soon as practicable. Means should be provided for undertaking the software maintenance in a way that ensures minimal downtime of the shipboard computer-based equipment or system.

7.9 The software maintenance should be assessed to determine and describe new functionalities, changes and improvements. A summary of new functionalities, changes and improvements should be provided to the Contracted Service Provider as necessary, and the Manufacturer should provide updates to maintenance and user manuals, where applicable.

7.10 Following completion of software maintenance, any feedback received regarding the result of the maintenance should, if appropriate, be addressed and used for improving maintenance procedures.

8 Guidance for the Contracted Service Provider and Certified Service Technician

8.1 The Contracted Service Provider should ensure that maintenance-related operations are carried out in accordance with a quality assurance system, covering, as a minimum:

- .1 competence management;
- .2 remote maintenance procedures, if applicable (see section 11);
- .3 reporting procedures;
- .4 shipboard operations safety briefing; and
- .5 cybersecurity.

8.2 Quality standards and internal training for Certified Service Technicians should be established by the Contracted Service Provider in line with maintenance and competency requirements of the Manufacturer and should be specified in a quality assurance system manual.

8.3 The cybersecurity competencies and internal cybersecurity training of Certified Service Technicians should be documented by the Contracted Service Provider, and should address:

- .1 general cybersecurity awareness, including system architecture, phishing attacks, password security, physical security, social engineering and remote working security;

- .2 integrity checking of removable media/storage devices; and
- .3 procedures for incident response.

8.4 The Contracted Service Provider should make the Manufacturer aware of any shortfall in performance of its Certified Service Technicians.

8.5 When planning the software maintenance, the Certified Service Technician, in consultation with the Company, should prepare a Plan of approach which should:

- .1 provide a description of the work expected to be undertaken;
- .2 be shared with and agreed to by the Company;
- .3 include information on any risks to the ship and shipboard equipment, alongside associated mitigations;
- .4 adhere to the HSE instructions provided by the Company, to ensure that the specific HSE requirements are known, understood and followed; and
- .5 include procedures for validating the operation of the shipboard computer-based equipment and systems after completion.

8.6 Where the Manufacturer has determined the need for a critical update and provided the necessary means, this software maintenance should be planned between the Contracted Service Provider and the Company to ensure that it will be undertaken as soon as practicable and that downtime of the equipment or system is minimized.

8.7 Before the Certified Service Technician arrives on board to perform software maintenance, the Contracted Service Provider should ensure that:

- .1 date, place and maintenance requirements, including port information and agent details, are planned and agreed with the Company;
- .2 the Certified Service Technician(s) is assigned to undertake the work, with the basis of the appointment documented and the certificate (paragraph 5.3 refers) shared with the Company;
- .3 information from the Company about the ship's equipment, system architecture, related configurations and software version(s) has been received and is sufficient;
- .4 a shipboard operations safety briefing for the Certified Service Technician(s) is undertaken to ensure that any specific requirements related to safety, security and environmental protection that have been communicated by the Company are understood;
- .5 the applicable software version(s) for the shipboard computer-based equipment or system are identified and prepared for installation;
- .6 the identity of the Certified Service Technician(s) assigned to undertake the work is forwarded to the ship for ISPS clearance and, where the assigned person(s) is subsequently unable to come on board, the Company is

- informed in advance about any replacement person(s) or about cancellation in case a Certified Service Technician is not available; and
- .7 all necessary tools and resources needed to access the shipboard computer-based equipment or system for software maintenance are prepared (for example: laptop, media device, specific tools recommended by the Manufacturer).

8.8 Where shipboard computer-based equipment and systems have been designed with recovery procedures, these should be utilized when required, for example if errors occur during software maintenance.

8.9 Procedures to protect against cybersecurity incidents during a software maintenance event should be agreed with the Company, including measures for demonstrating that removable media/storage devices have been checked for malware.

8.10 Uncontrolled equipment used during software maintenance, other than removable media/storage devices (as defined in these Guidelines), should not be directly connected to a controlled network. Such uncontrolled equipment should only be connected to a controlled network through a firewall or similar gateway device³.

8.11 In order to complete the software maintenance event, the Certified Service Technician should:

- .1 ensure that the equipment or system functions as intended after the software maintenance (subject to agreement with the Company, the Certified Service Technician may remain onboard to verify correct operation of the shipboard computer-based equipment during voyage);
- .2 where the shipboard computer-based equipment or system provides a mechanism to generate an on-the-spot diagnostic report, execute this process and include the report in the electronic service report;
- .3 complete and sign an electronic service report in accordance with section 6, and provide a copy to the Company for countersignature of the electronic service report by the representative of the Company and for inclusion into the onboard software log;
- .4 demonstrate in the presence of the ship's master and/or relevant crew member(s) that the shipboard equipment or system functions and operates as intended;
- .5 if applicable, demonstrate to the master and/or relevant crew member(s) any new/changed functionality; and
- .6 if applicable, provide updated user manuals to the ship.

8.12 Following completion of a software maintenance event, the Certified Service Technician should advise the Manufacturer of any issues or potential improvements to be considered for future software maintenance.

³ For example, IEC 61162-460 specifies a device called a "-460 Gateway" and a device called a "-460 Wireless gateway" for the purpose of connecting controlled and uncontrolled networks.

9 Guidance for the Company

9.1 The Company should ensure safe practices for the ship's safe navigation and operation during software maintenance and assess identified possible risks to the ship. Procedures should be in place to ensure that shipboard computer-based equipment and system software is maintained taking into consideration the guidance of the Manufacturer. Such procedures could, for example, include annual performance tests, clean-ups, diagnostics and instructions for when this should take place.

9.2 Where an operational anomaly or software defect has been identified on a shipboard computer-based equipment or system, the Company should provide the Contracted Service Provider with information concerning the equipment or the system, connections, related configurations and software versions, along with port information and agent details.

9.3 When planning a software maintenance event, the Company should prepare a procedure, taking into account the following considerations as well as the category and method of software maintenance:

- .1 identification of the need for additional familiarization, changes to operating procedures, and changes to onboard documentation;
- .2 description of how to avoid security risks including preventing unauthorized access, inappropriate assignment of user privileges, and spread of malware;
- .3 identification of the software, shipboard equipment, system and network to be maintained;
- .4 identification of all shipboard equipment and systems affected, taking into account the interface connections to the shipboard computer-based equipment and/or systems requiring the software maintenance;
- .5 identity of Certified Service Technician assigned to undertake the software maintenance;
- .6 preparation for remote access if this is agreed to be undertaken during the software maintenance (see section 12);
- .7 identification of appropriate crew member(s) to assist with the software maintenance; and
- .8 coordination with the master to ensure the safety of navigation during the software maintenance event.

9.4 During operational planning of a software maintenance event, the Company should ensure that:

- .1 date, place and maintenance requirements for the shipboard computer-based equipment or system, including port information and agent details, are planned and agreed upon with the assigned Certified Service Technician;
- .2 information is sent to the Certified Service Technician about the ship's equipment, system architecture, related configurations, and software version(s);

- .3 where the Manufacturer has determined the need for a critical update and provided the necessary means, the software maintenance is planned with the Contracted Service Provider(s) to ensure that it will be undertaken as soon as practicable and that downtime of the shipboard computer-based equipment or system is minimized;
- .4 any specific HSE instructions are communicated to the Certified Service Technician so that these may be adhered to in the Plan of approach; and
- .5 a copy of the Certified Service Technician's certificate(s) is/are requested.

9.5 Procedures should be in place to protect shipboard computer-based equipment and systems from malicious or unintentional security threats during software maintenance and they should include the following considerations:

- .1 identity of the Certified Service Technician coming on board to undertake the software maintenance; and
- .2 the Certified Service Technician access management.

9.6 When removable media/storage devices are used during software maintenance, the Company should ensure that the Certified Service Technician demonstrates that such devices have been checked for malware before the maintenance is carried out.

9.7 Each software maintenance event should be recorded in the onboard software log and linked to the associated electronic service report, in accordance with appendices 1 and 2. Such records should be made available on request to the Certified Service Technician in support of future software maintenance.

9.8 Following the conclusion of a software maintenance event, the master should be responsible for confirming that the shipboard computer-based equipment or system functions as intended.

9.9 On completion of a software maintenance event, the Company should advise the Contracted Service Provider of any issues or potential improvements to be considered for future software maintenance.

9.10 Following a software maintenance event, crew familiarization should be ensured for any new functionalities, changes or improvements.

10 Additional guidance for the Manufacturer – remote software maintenance

Shipboard computer-based equipment and systems that support remote software maintenance should:

- .1 provide multi-factor authentication to verify the identity of remote users;
- .2 have the capabilities necessary to manage interruptions to remote access sessions without compromising their integrity and availability;
- .3 provide measures to terminate a remote software maintenance event;
- .4 provide measures to ensure the integrity of the maintenance, including any data transferred; and

- .5 include programs to enable testing of the remote access feature, including functional tests and failure tests.

11 Additional guidance for the Contracted Service Provider and Certified Service Technician – remote software maintenance

11.1 Planning for remote software maintenance should be coordinated with the Company and the ship's master.

11.2 Remote software maintenance should only be carried out on shipboard computer-based equipment or systems connected to a controlled network.

11.3 Remote access to any shipboard computer-based equipment or system must only be carried out with the express permission of the Company. Additionally, permission should be obtained from the ship's master before initiating each remote software maintenance session.

11.4 The shore-side external access points of remote connections should be secured to prevent unauthorized access. Procedures to ensure the identity of the Certified Service Technician should be in place.

11.5 Where the remote software maintenance involves real-time communication and/or monitoring, the means of communication should be arranged between the Certified Service Technician and the ship before initiating the remote maintenance.

11.6 A time slot for when the shipboard computer-based system or equipment is connected and powered up should be agreed with the ship's master. After concluding the maintenance, procedures for how to determine when the shipboard connection can be closed should be agreed in advance.

11.7 The Plan of approach should document:

- .1 how the remote maintenance will be carried out in a safe and secure way including a description of the work expected to be undertaken, and any communications between the Certified Service Technician and the ship;
- .2 how all cybersecurity-related aspects of remote maintenance will be controlled from the start to the end of the remote software maintenance event, including but not limited to data integrity and security, access rights and operational state of the shipboard computer-based equipment or system;
- .3 the communications channel(s) to be used for the remote software maintenance event and its essential technical requirements (e.g. bandwidth);
- .4 what measures will be taken if the remote connection is lost or disrupted during the remote software maintenance event; and
- .5 how and in which circumstances the responsible crew member(s) on board can terminate the remote connection during remote software maintenance.

11.8 In the event of an error or disruption during the remote software maintenance event, an assessment will be conducted jointly with the Certified Service Technician, the ship and

the Company, as appropriate, as to whether the event should be continued with, or recovery procedures should be undertaken.

12 Additional guidance for the Company – remote software maintenance

12.1 Remote access should only be allowed to shipboard computer-based equipment and systems on a controlled network.

12.2 The remote access connection should be restricted to the shipboard computer-based equipment or system undergoing software maintenance.

12.3 For the purposes of planning and executing a remote software maintenance event, the Company should ensure that:

- .1 permission is provided to the Certified Service Technician to undertake remote maintenance, specifying who has access, when they have access, and what equipment they have access to;
- .2 permission is provided by the ship's master before every remote maintenance session;
- .3 procedures are in place to ensure that those service technicians certified to remotely access shipboard computer-based equipment and systems for the purposes of software maintenance can do so;
- .4 procedures are in place detailing the measures to be taken if the remote connection is lost or disrupted during the remote software maintenance event;
- .5 procedures are in place to ensure that remote software maintenance takes place during safe and suitable conditions; and
- .6 confirmation is received from the ship's master that the remote software maintenance event has been completed successfully.

12.4 In the event of an error or disruption during the remote software maintenance event, an assessment will be conducted jointly with the Certified Service Technician and the ship, as to whether the event should be continued with or recovery procedures should be undertaken.

APPENDIX 1

ELECTRONIC SERVICE REPORTS

This appendix specifies the minimum content of an electronic service report which is to be completed by the Certified Service Technician at the end of a software maintenance event.⁴

Format

The format of electronic service reports should be standardized, where practical, noting that its detailed content is dependent on the business system used by the Contracted Service Provider. The format of the electronic service report should be suitable for electronic filing and its content should be searchable. As a minimum, it should be possible to store these electronic service report documents in individual electronic folders.

Content

The following template identifies the minimum content of an electronic service report (pages should be numbered as, for example, 1 of 10):

"1 **General information**

Information about the ship:

- .1 Company name
- .2 Ship name
- .3 IMO number
- .4 MMSI

Information about the Contracted Service Provider and Certified Service Technician:

- .1 Name and contact information of the Contracted Service Provider
- .2 Name of the Certified Service Technician
- .3 Number and expiry date of the Certified Service Technician's certificate
- .4 Employee ID of the Certified Service Technician

2 Information about the shipboard computer-based equipment and software

For each piece of equipment and system undergoing software maintenance, the following details should be provided:

⁴ Refer to the most recent edition of the ISO 24060 series for requirements related to electronic service reports.

- .1 Manufacturer
- .2 Model (revision or edition number, if applicable)
- .3 Type
- .4 Serial number
- .5 Software version prior to maintenance
- .6 Date of previous software maintenance (installation date if no prior maintenance).

3 Details and purpose of the software maintenance event

- .1 Date and time of start of the software maintenance event;
- .2 Date and time of the end of the software maintenance event;
- .3 Location of the ship at the time of completion of the software maintenance event;
- .4 Method of software maintenance (onboard, onshore or remote);
- .5 Category of software maintenance (indicate as appropriate):
 - .1 Bug fix;
 - .2 Feature release;
 - .3 Compliance maintenance;
 - .4 Security update;
 - .5 Obsolescence maintenance;
 - .6 Combination of the above (specify);
 - .7 Other (specify); and
- .6 If it was a critical update (Yes/No).

4 Cybersecurity

The following information should be recorded for any removable media/storage device used to perform software maintenance:

- .1 Version and the make of the anti-virus/malware software used;
- .2 Last update of the anti-virus/malware database; and
- .3 Confirmation and date of clean anti-virus/malware scan.

5 Technical report

- .1 Detailed description of the work performed;

- .2 Outcome of the maintenance event; and
- .3 For each piece of equipment and system undergoing software maintenance, record the software version after completion.

6 Hardware changes

Should a hardware component of a shipboard computer-based equipment or system be added, removed or replaced, the following information should be recorded for the new hardware and any hardware that has been replaced:

- .1 Manufacturer;
- .2 Model (revision or edition number, if applicable);
- .3 Type; and
- .4 Serial number.

7 Operational status after software maintenance event

For each shipboard computer-based equipment and system undergoing software maintenance indicate [Yes]/[No]/[N/A] for the following:

- .1 all available self-test mechanisms have been completed successfully;
- .2 there was a demonstration in the presence of the ship's master and/or relevant crew member(s) that the shipboard computer-based equipment or system functions and operates as intended after the software maintenance;
- .3 additional new functionalities were demonstrated to the ship's master and/or relevant crew member(s);
- .4 an on-the-spot diagnostic report was generated after completion of the software maintenance event and is appended to the electronic service report; and
- .5 should a follow-up be deemed necessary (if yes, provide reasons/details).

8 Post-event acceptance

- .1 Has the software maintenance event been completed to the satisfaction of the ship's master? (Yes/No)
- .2 Capture feedback and comments from the ship's master and/or relevant crew member(s) about the software maintenance event.

9 Signatures

- .1 Certified Service Technician
- .2 Company representative.

Digital signatures that prevent tampering and confirm the originality of the content of the report should be considered."

APPENDIX 2

ONBOARD SOFTWARE LOG

1 The onboard software log is a repository of information relating to the software installed on shipboard computer-based equipment and systems, including associated software maintenance events and the related electronic service reports.⁵

2 Electronic service reports should be linked to individual software maintenance event records.

3 The onboard software log should be implemented and maintained by the Company and made available on board. The onboard software log should be updated after each software maintenance event.

4 Each onboard software log should include the following fields as a minimum:

.1 Ship details:

- .1 Ship name;
- .2 IMO number;
- .3 MMSI; and
- .4 Company name.

.2 Shipboard computer-based equipment or software details:

- .1 Manufacturer;
- .2 model (revision or edition number, if applicable);
- .3 type;
- .4 serial number;
- .5 previous software version;
- .6 current software version; and
- .7 software maintenance event details:
 - .1 date of the software maintenance event;
 - .2 initiator (Manufacturer/Contracted Service Provider/Company);
 - .3 method of software maintenance (onboard, onshore or remote);

⁵ ISO 24060-1 specifies requirements for a Ship Software Logging System (SSLS).

- .4 category of software maintenance;
- .5 status of equipment or system prior to software maintenance;
- .6 status of equipment or system on completion of software maintenance; and
- .7 Contracted Service Provider and Certified Service Technician details:
 - .1 name and contact information of the Contracted Service Provider;
 - .2 name of the Certified Service Technician;
 - .3 number and expiry date of the Certified Service Technician's certificate; and
 - .4 employee ID of the Certified Service Technician.

APPENDIX 3**ADDITIONAL SHIPBOARD COMPUTER-BASED SYSTEMS TO WHICH
THESE GUIDELINES MAY BE APPLIED**

1 These Guidelines may be applied, on a voluntary basis, to any shipboard computer-based system not included under paragraph 2.1 of these Guidelines.

2 A list of such systems is provided as follows (note that this list is not intended to be exhaustive):

- .1 alarm and monitoring systems for propulsion systems;
 - .2 ballast transfer valve remote control system;
 - .3 bilge level detection and associated control of pumps;
 - .4 bunkering control system;
 - .5 drilling systems;
 - .6 dynamic positioning system of equipment classes 2 and 3 according to MSC/Circ.645 on Guidelines for vessels with dynamic positioning systems;
 - .7 electric power system (including power management system);
 - .8 fuel oil treatment system;
 - .9 liquid cargo transfer control system;
 - .10 propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship;
 - .11 security, access control and surveillance system;
 - .12 ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in the operation of life-saving appliances equipment;
 - .13 ship to shore integrated systems (e.g. remote control systems);
 - .14 stabilization and ride control systems; and
 - .15 steering system control system.
-