CIRM Cyber Risk Code of Practice

for Vendors of Marine Electronic Equipment and Services

Edition 1.0
February 2020

Comité International Radio-Maritime (CIRM)
202 Lambeth Road, London, SE1 7JW, United Kingdom
Tel: +44 (0) 20 3411 8344
Email: office@cirm.org
www.cirm.org

DOCUMENT HISTORY

Version no.	Date	Details	Approved by
1.0	February 2020	First published version	CIRM Technical Steering Committee

TERMS OF USE

This Code of Practice ("CoP") has been prepared by Comité International Radio-Maritime (CIRM). Advice and information given in the CoP is intended purely as guidance, to be used at the user's own risk. No warranties or representations are given, nor is any duty of care or responsibility accepted by the Authors, their membership or employees of any person, firm, corporation or organisation (who or which has been in any way concerned with the furnishing of information or data, or the compilation or any translation, publishing, or supply of the CoP) for the accuracy of any information or advice given in the CoP or any omission from the CoP or for any consequence whatsoever resulting directly or indirectly from compliance with, adoption of or reliance on guidance contained in the CoP even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties.

TABLE OF CONTENTS

1. INTRODUCTION

The intended audience of the CIRM Cyber Risk Code of Practice ('the Code') is Vendors of marine electronic equipment and services; this includes Producers of shipboard Information Technology (IT) and Operational Technology (OT) equipment, System Integrators, Service Suppliers and Communications Service Providers in the marine electronics industry (collectively referred to hereunder as 'Vendors'). Vendors must understand the nature of cyber-attack threats and the vulnerabilities to those threats presented by their products and services, build in risk reduction measures, and help the shipowners, operators, crews and service personnel that buy and use their products to make good security decisions.

This voluntary Code is intended to be used:

- by CIRM member organisations to implement an effective and cost-efficient cyber security best practice derived from both the marine and other industries, and
- to promote CIRM's view of cyber security best practice.

Guidance on implementing the Code is provided in a companion document: CIRM Guideline GL-002.

2. PRINCIPLES OF THE CIRM CYBER RISK CODE OF PRACTICE

The foundation of Cyber Risk Management is a chain of trust.

Adequate cyber security for maritime actors is built on a common chain of trust, where every participant is responsible for providing the elements needed to establish adequate cyber security in their organisation, products and services, and thus together be able to provide a complete chain of cyber security.

To support this goal, the Code presents a set of guiding principles for all members of the stakeholder value chain to use in order to establish a provable chain of trust for a secure digital maritime environment.

All adherents to the Code will make best efforts to comply with the following principles:

1. **Adherence to applicable cyber risk standards, recommendations and guidance**
   - Consider cyber risk mitigation in the way that services and installations are delivered.
   - Deliver and maintain products and services with a defined level of cyber security and cyber resilience, for example by compliance with standards and recommendations provided by the International Maritime Organization (IMO), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and International Association of Classification Societies (IACS).
2. **Default cyber secure**
   - Set products and systems to a configuration mode in which the required implemented cyber security risk mitigations are enabled in their normal operating mode; i.e. if a configuration can be set in either a secure or non-secure mode, it will by default be set to the secure mode.

- Ensure that no hidden accounts are created. If accounts are needed for e.g. remote maintenance, the use of such accounts will be subject to awareness and agreement with the customer.

- Make customers aware of the impact of overriding or bypassing the security measures provided

3. **Confidentiality**

   - Treat customer's data and information related to cyber security and cyber security events as confidential, unless otherwise agreed with the customer.

4. **Quality as the foundation for cyber risk management**

   - Ensure that products and services are designed, developed and delivered using the principles and processes of a defined and accepted industry standard Quality Management System (e.g. ISO 9001)

5. **Software updates and vulnerability handling**

   - Make appropriate parties aware of the risk when any vulnerabilities that could affect the cyber security of a product or service are identified.

   - Use vulnerability information as an input to their risk assessments to determine the appropriate action.

   - Publicise dates after which support, updates and vulnerability handling for products and services they provide will no longer be available.

   - Share, either anonymously or openly, information with other stakeholder/adherents to the Code on emerging vulnerabilities, threats and cyber incidents in a timely and appropriate manner, to curtail or reduce the propagation rate and spread of malware.

6. **Continuous development**

   - Actively participate in CIRM activities related to the ongoing development of cyber security measures and industry standards.

3. GOVERNANCE

This Code and its related Guidelines will be maintained and governed by CIRM under the Cyber Risk Working Group. It will be reviewed and updated as needed.