|  |  |
| --- | --- |
| From: ARM | ????? |
| To: PAP | 27 October 2022 |

LIAISON NOTE

Cyber Security Awareness

# INTRODUCTION

ARM Working Group 2 has been working on Cyber Security topics in the IALA domain, in close collaboration with the other technical committees and with valuable input from the Cyber Security workshop in November 2021.

Two of the most relevant conclusions are that:

1. awareness of the need for cyber resilience in every (digital) system should be further improved, and
2. IALA products (Standards, Recommendations, Guidelines, etc.) should promote the principle of “security by design”, meaning that systems and communication should be developed with Cyber Security in mind and not applied as an “add-on feature” in a later stage.

A Recommendation on Cyber Security has been developed and a Guideline has been drafted (to be completed during work period 2023-2027). This will, however, not automatically lead to action within all Committees, Working Groups, Task Groups and other IALA activities and therefore, help from all chairs, vice chairs and the IALA secretariat is needed.

The ARM committee is available to provide assistance, on request, to any working group or task group, either by providing textual input or review, or by means of a (virtual) meeting.

# ACTION REQUESTED

All Committee chairs and vice chairs and all Working Group chairs and vice chairs are requested to:

1. when drafting a new Standard, Recommendation or Guideline, explicitly ask the author(s) if Cyber Security is relevant for the product and if a chapter or paragraph on the topic should be included;
2. when reviewing or revising IALA Standards, Recommendations or Guidelines, consider including a chapter or paragraph on the topic of Cyber Security;
3. call in the assistance from ARM, or an (external) subject matter expert if needed.

The IALA secretariat is requested to:

1. consider updating IALA templates to include standard topics (chapter/paragraph names), including a chapter or paragraph on cyber security/resilience, as a reminder for users of the template;
2. determine if output documents from committees may benefit from an (additional) review on Cyber Security.