IALA RECOMMENDATION (NORMATIVE)

R1024
CYBER SECURITY FOR THE IALA DOMAINS

Edition 1.0

December 2022

urn:mrn:iala:pub:r1024:ed1.0

10, rue des Gaudines – 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01 – contact@iala-aism.org

www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

DOCUMENT REVISION

Revisions to this document are to be noted in the table prior to the issue of a revised document.

Date	Details	Approval
December 2022	First issue	Council 76

THE COUNCIL

RECALLING:

1 the function of IALA with respect to Safety of Navigation, the efficiency of maritime transport and the protection of the environment.

2 Article 8 of the IALA Constitution regarding the authority, duties and functions of the Council.

RECOGNIZING:

1 that the maritime sector is increasingly depending on digital and (inter)connected technologies and systems.

2 that technologies applied for Maritime Services in the context of e-Navigation and AtoN, including VTS, may be susceptible to accidental and deliberate disruption.

CONSIDERING the endorsement of the ARM Committee of the findings of the IALA workshop on cyber security that was held from 15 to 19 November 2021 as a virtual workshop and several input documents on cyber security in various committees.

NOTING:

1 that awareness of cyber risk within the IALA domains and among the IALA members may be improved, especially for non-IT personnel;

2 that existing risk management processes often do not include cyber risks;

3 that the risk of unavailability or unreliability of systems due to cyber incidents is often not included in business continuity plans;

4 that there often is insufficient insight into used technology, especially legacy systems, within members environments;

5 that there are many tools, publications, standards, and best practices available to address cyber security vulnerabilities, risky processes, and human behaviours;

6 that specific technologies are used within the IALA domains for which there are no ready-to-use standards or best practices regarding cyber security; and

7 that the process of modernization is often lengthy and resource intensive.

RECOMMENDS:

1 to improve cyber security awareness:

a within IALA by providing practical technical examples and how such examples can be valuable for members, both in identifying their own cyber risks and in applying mitigation methods; and

b within the members organizations by supporting the performance of cyber security functions by all personnel, including management, through appropriate means, which may include policy development, training or exercises.

2 that IALA members develop or update their risk management processes and perform risk assessments where necessary, with prioritization of:

a physical safety risks stemming from vulnerabilities in digital systems and data handling;

b the estimation of impact, corruption or (accidental/deliberate) loss of critical systems or (corruption of) data following a cyber incident; and

c equipment and data receptive to vulnerabilities and cyber attacks.

3 to amend business continuity plans with cyber incident scenarios and mitigations as well as to develop incident response and - recovery plans;

4 that regular inventories be performed, including a risk assessment per (type of) system or technology used, with due consideration to the interconnections with other systems and data sources. Suggested methods are identified in Annex A;

5 to adopt appropriate industry standards for managing cyber risk and/or apply best practices. In particular, the concept of “security by design” should be practiced. Suggestions for appropriate standards and best practices are summarized in Annex A;

6 to implement protective measures or processes for all AtoN services and technologies, including VTS; and

7 that IALA members work towards the goal of ensuring all data in the IALA domain is provided with a means to authenticate the data, thereby allowing the user to determine if data originates from a legitimate source.

INVITES Members and Marine Aids to Navigation authorities to implement the provisions of the Recommendation.

REQUESTS the ARM committee to keep the Recommendation under review and to propose amendments as necessary.

ANNEX CONTENTS

ANNEX A SUGGESTIONS FOR APPROPRIATE STANDARDS AND BEST PRACTICES

1. INTRODUCTION

Cyber security is a relevant topic for all uses of digital technology, not only within IALA but everywhere around us. It is not an add-on technology, nor can it be handled separately from any work on digital technologies; it should be incorporated in all technology, process, and human behaviour.

Because of the broad spectrum of cyber security, many industry standards and best practices are available to address technical weaknesses, processes, and awareness in the IALA domains Maritime Services in the context of e-Navigation and AtoN, including VTS.

2. AVAILABLE STANDARDS AND BEST PRACTICES

The IALA workshop on cyber security, held virtually in November 2021, produced a list of available standards for adoption by IALA members. The workshop report elaborates on these standards, and they are summarized below.

2.1. GENERIC / IT

- ISO/IEC 27001 series: IT Information Security and Privacy Management, providing requirements for an information security management system (ISMS)
- NIST Cybersecurity Framework: guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk
- NIST SP800-53: Security and Privacy Controls for Information Systems and Organizations

2.2. OPERATIONAL TECHNOLOGY (OT)

- IEC 62443: Cyber security for Industrial Automation and Control Systems

2.3. FOR THE MARITIME DOMAIN

- IMO MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management
- ISO/IEC 63173: Maritime navigation and radiocommunication equipment and systems
- Resolution MSC.428(98): MSC Maritime Cyber Risk Management in Safety Management Systems
- NISTIR 8323: Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
- ISO 23806: Maritime Cyber safety standard
- BIMCO et al.: The Guidelines on Cyber Security Onboard Ships