Recommendation 11 : 2013 as amended by Recommendation 07: 2014

THE NORTH-EAST ATLANTIC FISHERIES COMMISSION AT ITS ANNUAL MEETING IN NOVEMBER 2012 ADOPTED, IN ACCORDANCE WITH ARTICLE 5 OF THE CONVENTION ON MULTILATERAL COOPERATION IN NORTH-EAST ATLANTIC FISHERIES, A RECOMMENDATION TO ADOPT AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR NEAFC

1. Objective

The objective of this recommendation is to establish, implement, operate, monitor, review, maintain and improve information security management within NEAFC.

2. Scope

This recommendation shall cover gathering, transmission, storage and dissemination of all information and data within NEAFC. This excludes the internal processes of the Contracting Parties.

The Information Security Management System (ISMS) of NEAFC consists of the following documents:

- This Recommendation[1]
- The Guidelines referred to in Articles 5, 6, 7.2, 8, 9, 10, 11, 12 and 14
- The Terms and Conditions referred to in Article 6.2

The security and confidentiality policy is based on the relevant parts of the ISO/IEC 27001 standard[2].

3. Risk management

NEAFC Committees and other subsidiary bodies shall prioritise the analysis and evaluation of risks. The Secretariat shall assist in this work. The risk analysis shall be reviewed annually and the result presented to the Commission.

4. Security policy

The information security policy of NEAFC is to use the ISMS to achieve an appropriate security and confidentiality focus in the organisation. ISMS documents shall be formulated by AGDC, unless otherwise specified, and proposed to the Commission. When the Commission adopts or amends an ISMS document, the Secretary shall publish and communicate this document to all Contracting Parties and other relevant parties.

This policy shall be reviewed on a regular basis, taking account of the analysis and evaluation of risks undertaken in accordance with the previous paragraph and, when changes are made to the ISO standard. AGDC shall in this context make proposals to the Commisson, as appropriate.

[1] Recommendations are legal instruments adopted by the NEAFC Commission.

[2] ISO/IEC 27001(First edition 2005 10/15) "Information technology – Security techniques – Information security management systems – Requirements"

5. Security guidelines

Information Security Guidelines shall be formulated by AGDC.
After formal approval by the Commission, the Secretary shall publish and communicate these Guidelines to all Contracting Parties and other relevant parties.

These guidelines shall be reviewed on a regular basis, taking account of the analysis and evaluation of risks undertaken in accordance with the previous paragraph.

6. Organisation of information security

6.1 Internal organisation

Each Contracting Party and the Secretary shall nominate a security system administrator. The security system administrators, in cooperation with other persons, groups and committees, shall manage information security within NEAFC, according to Guidelines on the Organisation of Internal Information Security. This will include promoting compliance with the security policies and acting as a liaison with the Secretariat on security matters. The Secretary shall maintain a list of theses security system administrators.

The Secretariat's security system administrator will raise awareness for the security policies within the Secretariat, coordinate security with service providers and external consultants, will manage confidentiality agreements, and will cooperate in any auditing of the information security system. The security system administrators may seek the advice of the AGDC as appropriate.

6.2 External parties

Terms and Conditions to allow access to certain information to the public shall be formulated by relevant subsidiary bodies and adopted by the Commission. The Secretary shall make them publicly available. These terms and conditions shall be reviewed on a regular basis.

Service providers and expert consultants may be given access to information according to the *Access Control Security Guidelines*. The Secretary shall ensure that when entering into contracts with third parties security and confidentiality issues are addressed.

7. Asset management

7.1 Responsibility for assets

The Secretariat shall maintain an inventory of NEAFC's relevant assets, including hardware, software and information, and ensure that security system administrators have access to this inventory. AGDC will review this inventory annually.

7.2 Information Classification

Information shall be classified as either public or restricted. The detailed rules for the management of public and restricted information shall be outlined in the *Information Security Guidelines*.

8. Human resources security

Human Resources Security Guidelines shall be put in place by the Secretariat to ensure that security roles and responsibilities of employees, contractors and third party users are defined and documented, consistent with NEAFC's information and security policy. These Guidelines shall be made available to Contracting Parties on request and reviewed on a regular basis.

9. Physical and environmental security

Measures to prevent unauthorized physical access, damage and interference to NEAFC's premises and information and to prevent loss, damage, theft or compromise of assets and interruption to NEAFC's activities shall be outlined in the *Physical and Environmental Security Guidelines*.

10. Communication and operations management

NEAFC *Communication and Operations Security Guidelines* shall contain measures to ensure the correct and secure operation of information processing facilities; the delivery management of third party services; to minimise the risk of system failures; to protect the integrity of software and information against malicious and mobile code; to deploy back up techniques to maintain the integrity and availability of information processing facilities; To ensure the protection of information in networks and the protection of the supporting infrastructure; To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities; To maintain the security of information and software exchanged within NEAFC and with any external entity; To detect unauthorised information processing activities.

11. Access control

NEAFC *Access Control Security Guidelines* shall contain measures to ensure appropriate controls to access information; To ensure authorized user access and to prevent unauthorized access to information systems; To prevent unauthorized user access, and compromise or theft of information and information processing facilities; To prevent unauthorized access to networked services; To prevent unauthorized access to operating systems; To prevent unauthorized access to information held in application systems; To ensure information security when using mobile computing and teleworking facilities.

12. **Information systems acquisition, development and maintenance**

NEAFC *System Acquisition, Development and Maintenance Security Guidelines* shall contain measures to ensure that security is an integral part of information systems; To prevent errors, loss, unauthorized modification or misuse of information in applications; To protect the confidentiality, authenticity or integrity of information by cryptographic means; To ensure the security of system files; To maintain the security of application system software and information; To reduce risks resulting from exploitation of published technical vulnerabilities;

13. **Information security incident management**

The security system administrators should ensure that security events and weaknesses associated with information systems are communicated to all security system administrators in a manner allowing for timely corrective action to be taken. System changes arising from such events should be dealt with by AGDC.

14. **Business continuity management**

The Secretariat shall undertake measures to counteract interruptions to activities and to protect critical processes from the effects of major failures of information systems or disasters and to ensure their timely reinstatement. These measures shall be described in the *Business Continuity Management Guidelines*.

15. **Compliance**

The Secretariat has the responsibility to comply with the relevant legal, regulatory and contractual obligations and standards.

The security system administrators shall ensure compliance of NEAFC practices with the Information Security Management System of NEAFC.

The Information Security Management System of NEAFC and its implementation should be subject to external audit on a regular basis.

AGDC shall review on a regular basis the compliance with ISMS of
NEAFC, as well as reports from the external audit.