Maritime & Coastguard Agency

Information Assurance

Security Aspects Letter

1 Summary

This Security Aspects Letter (SAL) states responsibilities for contractors and third parties with respect to the handling of MCA information and information processing facilities and is issued for the purpose of bringing attention to good security practice through the interpretation of and compliance with Her Majesty's Government (HMG) Security Policy Framework (SPF).

2 Subcontracts

Work that is subcontracted by the contracting authority is subject to the same requirements of the SPF and guidance stipulated in this SAL.

3 Security Measures

3.1 Unless explicit written authorisation has been received from the MCA neither the contracted company nor its employees shall disclose any aspect of MCA information, processes or procedure.

3.2 Unless explicit written authorisation has been received from the MCA the contracted company and its employees must take reasonable steps to ensure that:

- no photograph of MCA information is taken;
- no copy of or extract from any MCA information is made.

4 Personnel Screening

4.1 No person may have access to MCA information assets or information processing facilities unless they satisfy the requirement of Baseline Personnel Security Standard (BPSS).

4.2 Persons requiring administrative/raised privileges or domain access to MCA I&T systems must have successfully completed National Security Vetting.

5 Information processing equipment

Connection of non-MCA authorised removable media to MCA networks including USBs, personal smartphones etc. is prohibited without MCA authorisation.

MCA-authorised removeable media is available upon request which can then be connected to the MCA networks.

6 Classification of documents and assets

6.1 All information and hardware originating from or produced for the MCA (unless otherwise specified) will be classified as OFFICIAL. OFFICIAL information may not always be marked as OFFICIAL.

6.2 An additional caveat of SENSITIVE may be applied to indicate sensitivity or content. When used this will show as OFFICIAL-SENSITIVE. Further descriptors may also be applied to OFFICIAL-SENSITIVE information:

- PERSONAL;
- COMMERCIAL.

6.3 Information such as IP addresses, documentation relating to system design and architecture, system risks and vulnerabilities that had originated must be stored, processed, transferred and handled as OFFICIAL-SENSITIVE.

6.4 OFFICIAL-SENSITIVE information must be physically and electronically handled and stored in secure manner. All other OFFICIAL information must be handled and stored in a manner that is appropriate to its content and value.

6.5 OFFICIAL-SENSITIVE information cannot be emailed over the public internet or emailed from outside the MCA network(s) without the use of a secure email service.

6.6 Access to information or assets will only be granted to those who have a business need and have satisfied the appropriate clearances. Where applicable regular access to information assets will require a data sharing agreement to be put in place.

6.7 Casual access to sensitive assets is not permitted. If you have doubt regarding your access rights this must be reported to your MCA Contract Manager or Information Assurance (informationassurance@mcga.gov.uk) without undue delay.

6.8 You may handle information or documentation that has a historic marking of PROTECT, RESTRICTED or above. This information must be handled in the same way as OFFICIAL-SENSITIVE.

7 Information Handling

7.1 MCA information and assets must be handled and stored in such a way that all responsibilities under Information Legislation can be discharged (including but not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and the Freedom of Information Act 2000).

7.2 When handling MCA information you must ensure that:

- all information is securely stored at all times;
- work areas and desks are clear of sensitive information when not in use;
- information is adequately protected from unauthorised access;
- sensitive information must not be transmitted without encryption over the public internet. Contact MCA Contract Manager or Information Assurance **(**informationassurance@mcga.gov.uk**)** for further information;
- paper documents bearing an OFFICIAL – SENSITIVE marking and other sensitive (unmarked) documentation are shredded when no longer required using MCA approved methods;
- personal data is classified and handled as OFFICIAL. In very limited circumstances, specific considerations towards sensitivity may warrant additional controls to reinforce the “need to know” principle regarding access to certain personal data;
- the “need to know” principle is followed where applicable;
- users must be aware of their surroundings when discussing official and sensitive information.

8 Carriage of Information

The carriage of information off-site must be in accordance with the instructions of the MCA Contract Manager or Information Assurance.

For data migration, secure data migration and transfer advice must be followed. Please contact the Data Protection Manager (dataprotectionmanager@mcga.gov.uk).

9 Removal of Hardware

All removals of MCA hardware off-site must be in accordance with the instructions of the MCA Contract Manager or Information Assurance.

10 Access Control

Users with passwords to MCA assets and systems must:

- protect their password and never disclose them to others;
- never record passwords in clear text or in a manner identifiable by others;
- not attempt to gain access to an MCA network or information processing facility with log on credentials that are not their own;
- only access accounts for which approval is given;
- not use the same password for different accounts/assets;
- not use the same password for work and social accounts;
- change a password if it is believed to be compromised;
- inform IA and their Contract Manager if a password becomes known by another person. The password must be changed without delay.
- inform IA as soon as possible if a user is made aware of an unknown unsuccessful logon attempt.

11 Change Management

Contractors must not change or attempt to change the configuration of MCA systems unless specifically authorised by the MCA Contract Manager and managed in accordance with MCA Directorate of Information & Technology's Change Control procedure.

Records/authorisations must be maintained of all requested and actioned changes.

12 Installation of Software

The installation of software on MCA networks or information processing facilities is prohibited unless explicit authorisation has been received from the MCA Contract Manager.

13 Security Incidents

13.1 All actual or suspected security incidents must be reported to Information Assurance (informationassurance@mcga.gov.uk) and the MCA Contract Manager without undue delay.

13.2 All actual or suspected data incidents including accidental or unauthorised access, destruction, disclosure or transfer or other improper use of personal data must be immediately reported to the Data Protection Manager (dataprotectionmanager@mcga.gov.uk) and the MCA Contract Manager to allow the Maritime and Coastguard Agency to meet its obligations to notify the Supervisory Authority or any other regulatory or governmental authorities or Data Subjects of such events where we are required to do so by law.

14 Information and procedures

Further information and procedures are available from Information Assurance upon request.

15 Contact details

For further guidance please contact:

- Your MCA Contract Manager;
- Information Assurance - informationassurance@mcga.gov.uk;
- Data Protection Manager - dataprotectionmanager@mcga.gov.uk.

16 Consent

By signing below, the named third-party signifies that they have read and understood the Security Aspects Letter (SAL), that they are the responsible person within their organisation for all MCA activities and that they will circulate the SAL to all staff that work on/with the MCA's systems/data etc (signed copies are not required from each individual).

Signed copy from to be returned to IA - informationassurance@mcga.gov.uk

Company:	
Name:	
Job Title:	
Date:	
Signature:	