Ministry of Defence

Industry Security Notice

Number 2023/04

Subject: **Electronic Movement of OFFICIAL-SENSITIVE MOD Identifiable Information**

Introduction

1. This ISN outlines the requirements for managing the Information Security risks associated with the electronic movement of OFFICIAL-SENSITIVE MOD Identifiable Information (MODII)[1], both internally and externally over the Internet.

Status

2. This ISN replaces ISN 2022/09. The content has been updated as a result of feedback and remains valid until superseded or withdrawn.

Background

3. OFFICIAL-SENSITIVE is a limited subset of the 'OFFICIAL' classification that may attract additional measures in order to reinforce the 'need to know' principle. It is used to designate information that may have more damaging consequences (for individuals, an organisation or government) if it were lost, stolen or inappropriately disclosed[2].

4. Although within the OFFICIAL tier, OFFICIAL-SENSITIVE information must be

[1] As defined by ISN 2016/05 'Definition of MOD Identifiable Information'.

[2] Government Security Classification – May 18

securely managed by appropriate measures and meaningful handling guidance.

Action by Industry

5. Where OFFICIAL-SENSITIVE material is transmitted electronically, the following measures must be enforced together with any specific requirements imposed by the Information Asset Owner (IAO), Project Teams (PT) and/or Security Aspects Letter (SAL). Where the requirements within this document impose a more stringent requirement than those imposed by the IAO / PT / SAL, it shall take precedence.

Need-to-Know

6. The sender must ensure that any need-to-know requirements pertaining to the OFFICIAL-SENSITIVE material is enforced prior to the transmission of the material. This can be achieved by ensuring:

a. the recipient's email account is not subject to auto-forwarding, group access or delegated access[3]; and

b. the recipient understands any associated handling instructions or dissemination restrictions.

Marking

7. All OFFICIAL-SENSITIVE material must be appropriately marked. In addition to the labelling of documentation, transmission by email also requires one of the following methods of labelling:

a. use of inbuilt technical controls, such as Microsoft Azure Information Protection (AIP), to denote the classification of the transmission; or

b. manually constructing the email to clearly state:

   i. OFFICIAL-SENSITIVE, together with any additional descriptors (where applicable) within the subject line of the email; and

   ii. handling instructions or need-to-know requirements (where required) within the subject line or at the beginning of the body of the email.

Transmission requirements

8. The electronic transmission of MOD OFFICIAL-SENSITIVE material is permitted provided one of the following conditions is met:

---

[3] Unless the email is being sent to a designated inbox that is appropriate for receipt of OS information and all individuals with access to that email account have a NTK requirement of the information being sent.

a. The IAO provides written authorisation for the material to be transmitted without additional protection (as stated in points 6b to 6d below); or

b. The transmission of the material is conducted solely on a network accredited for OFFICIAL-SENSITIVE, for example via the Restricted LAN Interconnect (RLI); or

c. Recommended the end-to-end connection between the sender and receiver is configured to use mandatory TLS1.2 (or higher), but it is understood that opportunistic TLS is sometimes invoked, and this risk is accepted; or

d. The material is protected by Data at Rest (DAR) encryption, in accordance with the approved/acceptable[4] products outlined in ISN 2020/07 'Encryption of MODII at rest'[5]. Where this occurs, the associated password / encryption key:

   i. must meet NCSC requirements[6], with a minimum length of 9 characters;

   ii. must be sent to the recipient by an alternative method of communication than the encrypted file;

   iii. must preferably be sent to the recipient in two separate parts.

Personal Devices

9. OFFICIAL-SENSITIVE information must not be sent to a personal device[7] by email.

Validity / Expiry Date

10. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

11. The point of contact in respect of this ISN is:

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
email: UKStratComDD-CyDR-InfoCyPol@mod.gov.uk (Multiuser).

[4] The term 'Approved' means approved by NCSC. The term 'Acceptable' means approved under previous DIPCOG scheme but has been revalorised. In this context, the two terms mean the same but are used to distinguish the organisation that has assessed the product.
[5] For example, Zip encryption in AES-256 mode.
[6] Password policy: updating your approach - NCSC.GOV.UK
[7] Unless that personal device is included within a TOA as part of an accredited network.