Cabinet Office

Guidance: Protecting international RESTRICTED classified information

Version 1.3 – March 2020

Introduction

1. This guidance document is intended to assist HMG organisations and UK contractors who access, handle and/or store international classified information at the RESTRICTED level and no higher. This guidance should be read in conjunction with the relevant sections of Government Security policy, and for International Organisation RESTRICTED classified information the relevant security rules and regulations of that organisation. Contractors awarded international RESTRICTED classified contracts will also need meet any security provisions stipulated in their classified contract. If a classified contract has higher requirements that what is stipulated in this document then those provisions will generally prevail.

Access

2. International RESTRICTED classified information must only be accessed, handled, generated by, and discussed with other individuals who have a 'Need to Know'. The Need to Know principle essentially means that the dissemination of the RESTRICTED classified information should be no wider than is necessary for the efficient conduct of an organisation's business and, by implication, should be limited to those individuals who are appropriately authorised within an organisation to have access to it.

3. For British nationals no Personnel Security Clearance (i.e. National Security Vetting) is required for access to international RESTRICTED classified information.

4. Whilst no nationality restrictions are generally applicable at the international RESTRICTED level employers should be mindful of the Need to Know, any nationality sensitivities and any third party transfer restrictions before permitting access to this classified information.

5. Individuals who will require access to international RESTRICTED classified information must be briefed by their employer on their responsibilities for protecting sensitive information and be made aware of the relevant security rules and regulations in order to ensure this material is appropriately protected.

6. It is recommended, but not mandatory, that organisations holding international RESTRICTED material consider implementing and maintaining a register of their personnel who have been authorised to have access to the information in order to fulfil their duties.

Information management

7. International RESTRICTED classified information will be clearly and conspicuously marked by the originator upon creation. For a document, it will bear the relevant international RESTRICTED classification marking in the header and footer (centred) of each page, for example:

8. Only the originator (see next paragraph) of the international RESTRICTED classified information can decide whether the classification marking applied remains valid. If the holder of the RESTRICTED classified information is of the opinion that the marking is incorrect they will need to consult the originator.

9. The 'originator' of classified information can only be the Government or the International Organisation (e.g. NATO) that owns the information. Contractors can generate and create RESTRICTED information under contract, but are not considered as originators under security policy.

Control

10. UK entities holding international RESTRICTED assets at their facility should appoint an individual with responsibility and authority for ensuring security controls are maintained (i.e. a Security Officer). This appointed individual should assume responsibility for ensuring that employees who are entrusted with classified information understand their responsibilities and the organisation applies the necessary security controls.

11. It is recommended, though not mandatory, that organisations handling international RESTRICTED classified information record the movement of such assets in a register/database. This will help ensure such assets are properly accounted for within the facility, and can assist in security investigations should there be a security incident.

Handling

12. International RESTRICTED classified information can only be accessed and handled in a secure facility. Such a facility should have suitable controls and measures implemented to reduce the risk of information being accessed or overlooked by individuals without a Need to Know.

13. International RESTRICTED classified information cannot be left unattended in any place where someone without a Need to Know could access or overlook it. This information will need to be locked away in suitable office furniture when not in use, or locked in an office where there can be no access by unauthorised personnel.

14. International RESTRICTED classified information must not be read, discussed or worked on in public spaces (e.g. on public transport).

15. Only personnel who have a Need to Know can make copies of international RESTRICTED classified information. Copies should be kept to the absolute minimum necessary to fulfil a task and be appropriately destroyed when no longer required.

16. International RESTRICTED classified information will be at additional risk from compromise when it is physically transported between (or within) facilities so appropriate precautions should be taken to protect the information. International RESTRICTED classified information can be hand carried by staff between buildings, other sites within the UK, or to other facilities overseas, so long as the information is suitably covered in order to prevent inadvertent disclosure of the content (e.g. kept in an opaque folder or sealed envelope with no classification markings visible on outside).

17. If international RESTRICTED classified information is sent by post or by commercial courier service it generally has to be in two opaque envelopes (or other suitable packaging). The RESTRICTED classification marking will not appear on the outer envelope/packaging. The consignment should be addressed to a specific individual within the organisation, rather than the reception or a general office address. The outer envelope will also bear the full address of the sender in case delivery is not possible.

18. If sending international RESTRICTED classified information by postal or commercial courier service it is recommended that a service with a track and trace capability be used. It is also advised that the sender liaise with the intended recipient before the consignment is dispatched to agree a suitable date for delivery. This is to avoid the situation where the consignment cannot be delivered and has to be returned to the sender, or is held at a distribution hub, thereby increasing the risk of loss or compromise.

Information Assurance

19. An ICT system can only store and process international RESTRICTED classified information if that system has been appropriately accredited. During the accreditation process additional threats or increased risks may be identified which may be associated with the handling of the international RESTRICTED classified information. For the handling of International Organisation RESTRICTED assets the accreditor for the ICT system will need to consider the relevant security regulations, security policies and guidelines of that organisation. Unauthorised or non-official ICT (e.g. personal devices) is never permitted to be used to store and process international RESTRICTED classified information.

20. Cryptographic products used to protect international RESTRICTED on ICT and removable storage media will be either nationally approved or, for International Organisation RESTRICTED classified information, approved by that organisation. The NCI Agency lists NATO approved products. If a nationally approved cryptographic product is used for protecting International Organisation RESTRICTED classified information this will need to be compliant with the security rules and regulations of that organisation. The NCSC can provide advice if needed.

21. Unless there is a permitted exception, International RESTRICTED classified information cannot be transmitted over an unaccredited ICT system (e.g. in clear over the open internet) without using an approved cryptographic product or approved secure

mechanisms. If permitted under a General Security Agreement/Security Arrangement then this can only occur with the prior written consent of the originator.

22. International RESTRICTED classified information cannot be discussed over non-secure phone, mobile fax, or any other unencrypted channels.

Disclosure and release of international RESTRICTED classified information

23. International RESTRICTED classified information cannot be disclosed to the public or released to a third party without the prior written consent of the originator.

Destruction

24. When international RESTRICTED classified information provided is no longer required by an organisation it will need to be destroyed in such a manner that ensures it cannot be reconstructed. To that end, international RESTRICTED classified information will not be placed in unsecure bins (e.g. general office recycling points) where there is a risk of the information being accessed by unauthorised individuals.

Classified Contracting

25. Contractors may be obliged under contract to protect international RESTRICTED classified information generated or provided to them, usually through a Security Aspects Letter (SAL) and/or Programme Security Instruction (PSI). Contractors will follow the protective security requirements specified in that classified contract as well as abide by HMG security policy. In some instances the Contracting Authority of the classified contract may require security controls in excess of the baseline controls specified in HMG security policy; if so then the contractual obligations will generally prevail.

26. UK contractors do not require a Facility Security Clearance (FSC) to access, handle or store international RESTRICTED classified information at their facility.

27. Unless explicitly permitted under a classified contract, contractors will not let sub-contracts concerning international RESTRICTED classified information without first consulting and obtaining the written consent of their Contracting Authority.

Self-inspection and auditing

28. UK organisations that hold international RESTRICTED classified information should be self-inspected regularly by their local Security Officer/Facility Security Officer to ensure that the information is appropriately protected.

Security Incidents

29. UK organisations will investigate any case where it is known, or there are reasonable grounds for suspecting, that classified information originated and/or provided by an

international partner has been subject to a security breach, loss or compromise. UK contractors with a FSC will report any security incident to their HMG Security Controller, and UK contractors without a FSC will report any security incident to their relevant Contracting Authority.

30. In addition to the previous paragraph, significant security breaches that may lead to compromise of international RESTRICTED classified information, or a security incident where compromise of international RESTRICTED classified information has been confirmed (or is highly suspected), will need to be reported to the UK National Security Authority (UK NSA) without delay.

31. Notwithstanding the previous two paragraphs, a RESTRICTED level classified contract may also contain specific provisions concerning how security incidents should be reported. In case of conflict with this guidance, the requirements stated in a classified contract will generally prevail.

32. Any individual or organisation responsible for a breach of security rules and regulations may be liable to sanctions and/or legal action in accordance with the applicable national laws and regulations.

Annex A: Version History

Document Version	Date Published	Summary Of Changes
1.0	April 2014	First version published on GOV.UK.
1.1	July 2014	See version 1.1 for record of changes
1.2	November 2016	See version 1.2 for record of changes
1.3	March 2020	• References to SPF removed • Paragraph 1 – Reinforcing that contract provisions take priority over any guidance in this document. • Paragraph 3 - Reference to BPSS removed. • Paragraph 9 - Added to address originators. • Paragraph 17 – Corrected text to say there must be two envelopes. • Several other editorial changes • Version history now Annex A

Any enquiries regarding this publication should be sent to GSSmailbox@cabinet-office.gov.uk
You can download this publication from www.gov.uk.