Guidance 1.3- Working at TOP SECRET

What is TOP SECRET classified information?

1. The TOP SECRET classification tier is reserved for the most sensitive information assets that directly support or inform the national security of the UK or its allies AND require extremely high assurance of protection from the most serious threats, with the use of Secure Isolated Networks and highly secure physical infrastructure.

2. A compromise of TOP SECRET information could cause exceptionally grave damage. It could cause widespread loss of life or threaten the security or economic wellbeing of the UK or friendly nations. The expected capability level of hostile threat actors is extremely high at this tier.

3. The information creator must assess the potential impact of a compromise of information and the expected threat profile to determine whether information is TOP SECRET. The exceptionally grave damage of a compromise of information, combined with the enhanced capabilities expected from the most capable and well-resourced threat actors, is what defines TOP SECRET classified information.

Application of the TOP SECRET classification tier

4. The information creator is responsible for marking TOP SECRET information, which must only be used for the most sensitive assets. Before users can access TOP SECRET material for the first time, they must be briefed by their organisation's security team on how to handle the information and any related equipment in a careful and secure manner. It is the responsibility of organisations' security teams to ensure their users have routine refresher training thereafter. There is additional physical, personnel and technical guidance available for the TOP SECRET tier held at a higher classification. This is available from the Government Security Group; users should contact their security team for more information. The NCSC should be consulted where there is a business need for further guidance.

Application of the TOP SECRET baseline behaviours

5. TOP SECRET information justifies the most stringent behavioural, procedural and technical controls to protect against the highest capability of threat actors and to reduce the risk of an intentional or unintentional compromise. A set of security behaviours for users working at TOP SECRET is outlined in the table below. These should form the basis for the development of organisational security controls (alongside the controls table found in Guidance 1.5: Considerations for Security Advisors).

6. Organisations have the authority to develop security controls above the TOP SECRET baseline to manage specific risks. In addition, it is recognised that macro-level controls adopted by organisations can achieve equivalent or greater security outcomes, potentially allowing for variances 'below' the TOP SECRET baseline without compromising the overall protection of TOP SECRET information. However, such variances from the TOP SECRET baseline must be formally agreed by the Government Chief Security Officer, and the organisation will be required to demonstrate that the overall protection of TOP SECRET information is not compromised as a result.

7. At TOP SECRET, information handling and security requirements must be clearly communicated to recipients, and all recipients must have a strict need-to-know.

8. If additional security controls are necessary at a local level to manage specific risks, the information creator should consult with their SSA/SA or equivalent to ensure the controls are aligned with organisational policy and proportionate.

TOP SECRET classified information (Tier 3)	
Baseline behaviours and measures:	
Verbal information	**Meetings & Discussions:** ● The chair must make it clear before the meeting starts that TOP SECRET information will be discussed; assure that all attendees have the appropriate clearance; and, make clear any limitations or restrictions around further dissemination. ● Discuss only on IT or telephone systems approved by your organisation for use at TOP SECRET. ● In the office: ○ Use TOP SECRET accredited meeting rooms so conversations cannot be overheard. TOP SECRET environments can be assured against audio leakage and suitability to hold conversations. Contact UK NACE for guidance. ○ Use headphones (approved by your organisation) where possible. ○ Personal or corporate communication devices, wearable technology (such as smart watches) and smart listening devices (e.g. voice activated speakers) are prohibited from TOP SECRET areas, unless specifically approved by your organisation. ○ Meeting attendees can brief back to their team members with the appropriate clearance based on the need-to-know principle, but should check with the information creator if sharing further and should only brief staff in a suitably secure area for processing TOP SECRET. Where the information is not for further dissemination (even within teams) the chair should make this clear at the start of the discussion. ○ Technical surveillance counter-measures (counter eavesdropping) sweeps should be undertaken periodically to ensure the integrity of the meeting space.

	• Items entering a TOP SECRET area such as furniture should be sourced appropriately and, if necessary, inspected for sign of tamper. • In public: ○ Do not discuss.

Hard copy information	**Storage & Access**
	• In the office:
	  ○ Do not leave TOP SECRET material unattended.
	  ○ Store hardcopy information in NPSA approved physical security equipment approved for TOP SECRET when not in use.
	  ○ Print on corporate systems or devices approved by your organisation for use at TOP SECRET. You should consider printing TOP SECRET documents on yellow paper to make documents easier to recognise (in conjunction with your organisation's accessibility and sustainability guidance).
	  ○ Documents that are printed must be tethered together and bear a copy number on the top right corner of the first page (e.g. 1 of 3, 2 of 3, etc).
	  ○ Register information in the Protected Document Registry book (or equivalent), noting the reference number on each TOP SECRET document. Guidance on the use of Protected Document Registry books can be found in Guidance 1.5: Considerations for Security Advisors
	• At home:
	  ○ Remote working from home at TOP SECRET is not permitted.
	• Mark all information with "TOP SECRET" in the header and footer.
	  ○ If TOP SECRET information is to be shared with an international partner, the 'UK' prefix must be added at the front of the marking before it is provided.
	• Mark any files or groups of documents with the highest classification marking of the document pack.
	• Handwritten notes containing TOP SECRET information should be avoided. If they need to be taken, they

	must be treated the same as any other TOP SECRET document. **Transportation** ● Do not take TOP SECRET information home under any circumstances. ● Where possible, print TOP SECRET material securely at the destination rather than transporting hard copy material between HMG or cleared contractor sites. ● If documents must be moved from the office: ○ Conduct a Threat and Vulnerability Risk Assessment to understand risks relating to moving the documents and how to mitigate these risks; ○ A clear rationale must be set out in writing; and ○ Senior management (SCS1) and SSA/SA approval is needed, unless this has been delegated to other officials in line with local organisation policy. ● Strictly limit knowledge of planned movements to those with a need-to-know and the appropriate clearance. ● Check the document out in the Protected Document Registry book whenever transporting TOP SECRET documents. ● Moving physical assets by hand in the UK: ○ DV clearance as a minimum is required for carrying assets by hand. ○ Never access or read the information in public. ○ Two people (both cleared to DV) must escort the assets (unless within a specified Government Secure Zone). ○ Package documents in robust and opaque double envelopes or other suitable packaging. Only use tamper-evident packaging approved by NPSA in the Catalogue of Security Equipment (CSE). ○ Mark TOP SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.

	○ Add a return address and user contact details on both the inner and outer envelope/packaging in case the package is lost or misplaced. ○ Include a delivery receipt in the inner envelope/packaging. This delivery receipt must be returned immediately by the recipient. ○ If carrying by hand outside of a government building, place assets inside a discreet, opaque and locked security container. ● Moving physical assets by commercial courier service/postal service domestically (i.e. from and to a UK postal address) is not permitted. An SA/SSA approved secure mail delivery service that has two DV cleared escorts should always be used. ● Moving physical assets overseas: ○ Seek approval from the information creator, the SSA/SA and senior management (SCS1) before sending assets by post overseas, unless this has been delegated to other officials in your organisation's local policy. ○ Package documents in robust and opaque double envelopes or other suitable packaging. Only use tamper-evident packaging approved by NPSA in the CSE. ○ Mark TOP SECRET on the inner envelope/packaging, do not mark the outer packaging. ○ Include a delivery receipt in the inner envelope/packaging. This delivery receipt must be returned immediately by the recipient. ○ Use an approved government courier service e.g. diplomatic bag or military courier (defence courier service). **Destruction** ● Do not destroy assets without written approval from the information creator. Assets must be returned to the information creator in the first instance (unless written approval is given to the recipient to destroy the information in line with organisational policy). ● Dispose of information in the office in accordance with the NPSA Secure Destruction Standard. Use

	products from the CSE. Use an approved shredder. ● Destroy with a witness present (who also must be DV cleared). The person destroying the document and the witness must record the destruction in the Protected Document Registry book.
Electronic information	**Storage & Access** ● Only work in areas authorised by your organisation for processing TOP SECRET in the office using approved equipment. ● Never access or read TOP SECRET material in public or in the presence of unauthorised personnel. ● Mark all information with "TOP SECRET" in the header and footer, and number each page. ○ If the information is to be shared with an international partner the 'UK' prefix must be added at the front of the marking before it is provided. ● Only draft, store or share electronic information on IT systems approved by your organisation for use at TOP SECRET. It is <u>prohibited</u> to store TOP SECRET information on any system or device not specifically approved for TOP SECRET. This includes the corporate IT system for OFFICIAL or SECRET and personal devices. ● Lock devices when leaving your workspace for any length of time, even briefly. **Emails** ● Do not send information outside the Secure Isolated Network. ● Do not share with anyone outside your organisation without authorisation from the information creator and without need-to-know. ● Use clear handling instructions in the subject line and body of the email where appropriate. **Destruction** ● Dispose of digital information in the office in accordance with the NPSA Secure Destruction Standard and

	using products from the CSE. Also see the NCSC's 'Secure Sanitisation of Storage Media' guidance.