Guidance 1.2 - Working at SECRET

What is SECRET classified information?

1. The SECRET classification tier is used for sensitive information that requires enhanced protective controls, the use of appropriately assured IT (such as the Rosa capability provisioned to most HMG organisations) and heightened user discretion to guard against compromise.

2. SECRET information is much more sensitive than OFFICIAL information. Due to the sensitive nature of SECRET information, the threat profile anticipates the need to defend against a higher level of threat actor capability than would be typical at the OFFICIAL level. A compromise of SECRET information has serious implications. It could: threaten the lives of individuals or groups; and/or seriously damage the UK's security resilience, international relations, financial security; and/or, impede the UK's ability to investigate serious and organised crime.

3. Nonetheless, SECRET information still needs to be shared readily and promptly across HMG, the wider public sector and international and commercial partners; albeit using strict need-to-know principles. SECRET information is often time critical and needs to be operationalised - for example, 'action on' intelligence, trade negotiations, counter-terrorism and organised crime, military operations or sensitive defence equipment procurements. Information creators should be mindful of not over-classifying information to TOP SECRET, which may restrict the ability to share it as readily and promptly across HMG.

4. The sensitivity of SECRET information and the risks associated with its compromise need to be balanced against the risks of not sharing the information with colleagues who have a genuine need-to-know. Consequently, the associated baseline security behaviours and protective controls need to be agile and innovative, incentivising the right user behaviours, such as: exercising situational awareness; being accountable for security decisions and classifying correctly.

5. The information creator is responsible for assessing the potential impact of a compromise of information and the expected threat profile to determine whether information is SECRET. The serious impact of a compromise of

information, combined with the enhanced risks expected from highly capable threat actors, is what defines SECRET classified information.

Application of the SECRET classification tier

6. The information creator is responsible for marking their information, as well as monitoring and assessing whether any situational factors surrounding the information warrants updating the classification. Everyone who processes SECRET information assets on behalf of HMG (staff, delivery partners and third-party suppliers) is personally accountable for handling, disseminating and disposing of the information responsibly in line with HMG policy.

7. Users working on SECRET information, whether in the office or at home (or in exceptional circumstances away from the office or home), should be briefed by their security teams on their responsibilities in the handling of SECRET information and equipment in a careful and secure manner. There is additional physical, personnel and technical guidance available for the SECRET tier. This is available from the Government Security Group or the relevant organisation; users should contact their security team for more information.

8. Some information may only be classified as SECRET for a set (possibly short) period of time. The sensitivity of information can evolve through its life cycle e.g. information detailing a closely-held sensitive public announcement might be classified as SECRET until it is announced, but be OFFICIAL from the moment of announcement.

9. It is the information creator's responsibility to reclassify and remark the material if the context around an information asset has changed. Reclassifying material over its life cycle is important; it can avoid the proliferation of data assets requiring unnecessary security controls and resources, which is burdensome and expensive. It is also the responsibility of the information creator to inform previous recipients if classified information has been downgraded to OFFICIAL. In such circumstances, information creators should also consider whether additional markings apply to the downgraded information (such as -SENSITIVE).

10. The development of modern technologies, in particular cross domain capabilities, has created new ways in which staff can work at SECRET. For example: from a SECRET domain, importing and exporting data at OFFICIAL and browsing OFFICIAL networks and the internet. Small form factor crypto

devices also provide for remote and mobile ways of working with laptops, mobile phones and tablets - the security of which rely heavily on users exercising appropriate discretion, not least to ensure they are not overlooked or overheard[1]. Users must complete any mandatory training for their organisation's SECRET accredited technology before they first use their device(s) to access SECRET information.

Application of the SECRET baseline behaviours

11. The potentially serious impacts of a compromise of SECRET information, combined with the heightened threat profile, justifies enhanced (but proportionate) security behaviours and controls when compared to OFFICIAL. A set of baseline behaviours for users working at SECRET is outlined in the table below. These baseline behaviours should form the basis for the development of organisational security controls (alongside the controls table found in Guidance 1.5: Considerations for Security Advisors).

12. Organisations have the authority to develop security controls above the 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 SECRET baseline without compromising the overall protection of SECRET information. However, such variances from the 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 SECRET information is not compromised as a result.

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

14. In certain circumstances where there are heightened risks, it may be appropriate at a local level to apply additional protective security controls above the SECRET baseline behaviours to specific information assets. In such circumstances, the information creator should consult with their SSA/SA or equivalent to ensure that the proposed additional controls are aligned with organisational policy and proportionate.

[1] Noting that it is prohibited to do so when processing international partners' SECRET material.

SECRET classified information (Tier 2)	
Baseline behaviours and measures:	
Verbal information	**Meetings & Discussions:** ● Discuss only on IT or phone systems approved by your organisation’s SA/SSA for use at SECRET. ● The chair of the meeting must make it clear before the meeting begins that SECRET information will be discussed, ensure everyone present has the appropriate clearance, and should make clear any limitations or restrictions around further dissemination. ○ In public: Do not discuss. ○ In the office: Use meeting rooms so conversations cannot be overheard and use headphones (approved by your organisation) where possible. ○ If working remotely: Discuss using devices issued by your organisation for use at SECRET and use a private environment where conversations cannot be overheard by unauthorised personnel. Use headphones approved for use with the SECRET system. ○ Do not work on SECRET devices or work at SECRET in the presence of unauthorised personnel, or staff with the appropriate clearance but without a need-to-know. ● Do not discuss if there are any smart listening devices in the room (e.g. voice activated speakers), and remove all personal communication devices and wearable technology (such as a smart watch) from the room unless expressly risk assessed and permitted by an individual organisation or information system owner, or the devices vulnerabilities are mitigated with suitable personal communications devices audio countermeasures. ● Organisations should also consider carrying out periodic technical surveillance countermeasures (counter eavesdropping) sweeps of controlled office areas that frequently host SECRET meetings. ● Meeting attendees can brief back to their team members with the appropriate clearance based on the need-to-know principle, but they should check with the information creator if sharing further and should

	only brief staff in a suitably secure area for processing SECRET.
Hard copy information	**Storage & Access** ● In the office: ○ Store hardcopy information in National Protective Security Authority (NPSA) approved physical security equipment for SECRET. ○ Print on corporate systems or devices approved by your organisation for use at SECRET. You should consider printing SECRET documents on pink coloured paper in certain environments to make them easier to recognise (in conjunction with your organisation's accessibility and sustainability guidance). ○ Documents that are printed must bear a copy number on the top right corner of the first page (e.g. 1 of 3, 2 of 3, etc). ○ SECRET information must be registered in the Protected Document Registry book (or equivalent) if being kept for more than 5 days. ● Working remotely: ○ Do not remove hard copies of SECRET information from the workplace, except in exceptional circumstances for remote work. Where it is necessary to work on hard copy SECRET information at home or some other remote working site, senior management (SCS1) and SSA/SA approval must always be obtained in advance, unless this has been delegated to other officials in line with local organisation policy. ○ Always log in the Protected Document Register book (or equivalent) that hardcopy SECRET information is being taken out of the building. ○ Hard copy SECRET information must be kept in your possession or stored securely at all times when working remotely. ○ Store hardcopy information and devices in approved tamper evident containers in physical security equipment / furniture provided by your organisation. Containers should be placed in a discreet

location and checked regularly for tampering.

- Mark all information with “SECRET” in the header and footer and number each page.
  - If the 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.
- Wherever possible, handwritten notes containing SECRET information are to be avoided. If they need to be taken, they must be treated the same as any other SECRET document.

Transportation

- Where possible, print 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 the risks and how to mitigate them.
  - Senior management (SCS1) and SSA/SA approval must always be obtained in advance, unless this has been delegated to other officials in line with local organisation policy.
- 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 hardcopy SECRET documents.
- Moving physical assets by hand:
  - SC clearance as a minimum is required for carrying assets by hand.
  - Never access or read the information in public.
  - Risk assess the need for two people to escort the assets.
  - Tether pages together and number each page.
  - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
  - Mark SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.
  - Add a return address on both the inner and outer envelope/packaging.

    - Place assets inside a discreet third bag, or other suitable security container (e.g. locked briefcase) if carrying by hand outside of a government building.
- Moving physical assets by courier service/postal service domestically (i.e. from and to a UK postal address):
    - Include a return address on both the inner and outer envelope/packaging.
    - Include a delivery receipt in the inner envelope/packaging.
    - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
    - Mark SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.
    - Seek approval from senior management (SCS1 or above) and/or the SSA/SA before sending assets by commercial courier/post in the UK, unless this has been delegated to other officials in line with local organisational policy.
    - Use a commercial mail courier service with track and trace service or a government courier approved by your organisation, or contact the SSA/SA for guidance.
- Moving physical assets overseas:
    - By default, physical SECRET assets should be sent to the local Embassy/Mission using the diplomatic bag or military courier. Alternatively staff can consider accessing the SECRET assets electronically using accredited IT systems at the local Embassy/Mission.
    - Moving assets by hand carriage should only be considered in urgent situations where there is a clear business case and if permitted by the organisation under their internal rules.
    - Seek approval from the information creator and the SSA/SA before sending SECRET assets overseas, unless this has been delegated to other officials in line with local organisation policy.
    - Mark classification on the inner envelope/packaging. Do not mark the outer packaging with the classification level.
    - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
    - SC clearance as a minimum is required for carrying assets by hand.

Destruction

	● Always dispose of information in the office in accordance with the NPSA Secure Destruction Standard with products from the Catalogue of Security Equipment (CSE). ● Record destruction of hardcopy SECRET in the Protected Document Registry book.
Electronic information	**Storage & Access** ● Do not access SECRET material in public or in the presence of unauthorised personnel. ○ In the office: Only work in areas authorised by your organisation for SECRET or above. Do not work at SECRET in areas where there is a significant footfall of external visitors to the organisation and/or staff members without appropriate clearance. ○ Working remotely: Do not work where unauthorised co-residents, visitors or passers-by can overlook the information. ● Only draft, store or share electronic information on IT systems approved by your organisation for use at SECRET or above. Never store SECRET information on the corporate IT system for OFFICIAL or on personal devices. ● When away from your device or terminal, even for a short time, ensure it is locked and remove any key or Crypto Ignition Key (CIK). ● Working Remotely: ○ Avoid taking SECRET laptops to locations other than your home or workplace. ○ Always be discreet when using or transporting SECRET accredited devices, especially in publicly accessible locations and even when using secure containers. ○ Do not leave SECRET accredited laptops and mobile devices unaccompanied in locations which can be accessed by unauthorised personnel e.g. cars, coffee shops, or hotel rooms. Remove any token or CIK and keep discreetly in your possession separately from the device. Mobile devices should either be in your possession or in a secure container at all times. ○ SECRET accredited devices must be secured in a secure container or furniture provided for this purpose by your organisation when not in use. ○ Do not access SECRET IT systems via public Wi-Fi.

	● Mark all information with “SECRET” in the header and footer. ○ 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. ● Do not use IT equipment if there are any smart listening devices in the room (e.g. voice activated speakers), and remove all personal communication devices and wearable technology (such as a smart watch) from the room unless expressly risk assessed and permitted by an individual organisation or information system owner, or the devices vulnerabilities are mitigated with suitable personal communications devices audio countermeasures. **Emails** ● Do not send information outside the Secure Isolated Network (e.g. do not send via an OFFICIAL email account or via the open internet) ● Do not share with anyone within or outside your organisation without the need-to-know and the appropriate clearance. ● 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 with products from the CSE and the NCSC’s ‘Secure Sanitisation of Storage Media’ guidance.