Guidance 1.4 - Working Remotely at OFFICIAL and SECRET

1. Remote working is where users work either partially or entirely away from their organisation's principal sites in the UK. Hybrid remote working models have become the norm rather than the exception for many personnel across government and other organisations. From a security perspective, this flexibility creates different and often complex risks when compared to office working, which have to be managed.

2. Access to technology in government can enable users to work outside of the traditional office environment at both OFFICIAL and SECRET. Working remotely, however, places greater responsibility on the user to understand the risks to the information they are handling and relies on the user applying sound judgement through the right security behaviours.

Remote working: risks

3. Working outside of an office, without the enhanced protections of secure government infrastructure, creates additional risks to users and the classified information they are handling and for which they are responsible. Users must be mindful of the different contextual risks when transporting, working with, and storing government classified information remotely, as each situation poses unique challenges. Remote working increases the risk of loss or theft of classified information when accessing, transporting and storing it. This is because remote working creates additional or increased vulnerability to:

    a. The overlooking or overhearing of classified information by any unauthorised personnel or smart electronic devices. 'Unauthorised personnel' can include any member of the public, even known individuals such as housemates, friends or family members.

    b. Tampering with equipment, IT or information by unauthorised personnel, where assets are left unattended.

    c. Targeted compromise by threat actors, both physically and digitally.

4. Users are responsible for ensuring that proportionate security measures are in place to protect the information they have access to when working remotely.

Remote working requirements

5. Everyone who works for the Government has a personal responsibility for protecting the HMG information and assets which they have access to, and/or which is under their custody, regardless of their work location. When working remotely, users must protect information to the same standard as working in the office, if not a higher standard to manage the additional risks. There are some key considerations for users when working with classified information remotely:

    a. Consider the remote working environment in terms of the risks it presents (e.g. people overseeing work emails and documents; the risk of leaving physical documents in a public place), and take steps to address them. Very occasionally, at OFFICIAL a formal risk assessment may be considered appropriate in certain situational contexts. This should be stipulated by an organisation's local organisational policy.

    b. Access classified information via corporate IT, rather than hard-copy documents. Hard-copy documents must only be taken outside the office in exceptional circumstances with the appropriate approval for information of that sensitivity.

    c. Avoid drawing attention to the fact that HMG information is being transported or worked on.

    d. Complete the associated training for organisations' approved technology for working remotely.

6. Contractors working on contracts requiring them to operate at SECRET outside of Government facilities are subject to Facility Security Clearance (FSC) arrangements. It is for the HMG Contracting Authority's Security Advisor to risk assess, and approve or otherwise, SECRET working outside facilities specified by the relevant contract.

7. Further guidance on remote working for Contractors covered by FSC (List X) is available within the Security Requirements for Facility Security Clearance.

Remote working controls

8. This section covers protective security controls that users must follow when working remotely at home, flexibly and internationally. These three broad categories are non-exhaustive, but will likely cover most scenarios in which

users could be working with classified assets. The protective controls for remote working are driven by the same factors that underpin office working: sensitivity of the asset, the likelihood of compromise and the need-to-know principle.

9. Users should follow their organisation's local policy for remote working where one is in place and remote working is permitted.

Home remote working

10. Home working is defined as working at the user's home address registered with their organisation. Users are responsible for understanding the specific risks present in their home environment and securing the remote working location appropriately. Each user's home environment may vary: the risks posed to users living in shared accommodation with other household members will be different to those living on their own.

11. A user's permanent home address may change at short notice due to personal circumstances (such as to care for a family member). The user is responsible for understanding any specific security risks whilst working in the new location.

12. Users must follow the baseline behaviours outlined in Guidance 1.1: Working at OFFICIAL and Guidance 1.2: Working at SECRET, to protect OFFICIAL and SECRET classified information at home. In addition, Users must be especially mindful of other unauthorised residents and visitors without a need-to-know (e.g. friends, family members, housemates and any other member of the public) who could have access to their home working environment. Under no circumstances must someone without the appropriate level of security clearance and need-to-know access government classified information.

13. Users should review their risk assessments and discuss with their organisation's security team if they have contractors carry out renovations or maintenance in their home working environment when working with SECRET classified information.

Flexible remote working

14. Flexible remote working is defined as working from anywhere other than the user's permanent office, their organisation's principal sites or the user's home address registered with their organisation. Users working in alternative locations are often working in unfamiliar environments e.g. a hotel or

commercial shared workspaces. These environments can present additional risks, including being more freely accessible to people without the appropriate clearance and need-to-know.

15. A local organisational policy must outline any approvals required for users to access or take classified assets to locations beyond their permanent office, their home address or their organisation's principal sites. This policy should reflect broad scenarios that users will routinely encounter in their professional duties and personal lives e.g. visiting friends and family, and holidays. Users must not access or take classified assets with them abroad unless agreed with their line manager, HR and security team.

16. Users who have approval to undertake flexible remote work at OFFICIAL or SECRET in the UK should follow all of the flexible remote working behaviours in the table below and (as appropriate) the baseline security behaviours outlined in Guidance 1.1: Working at OFFICIAL and Guidance 1.2: Working at SECRET.

17. Working with SECRET information requires additional security awareness from users, especially when working remotely away from home. Users must think carefully beforehand about how the risks to SECRET information will be managed in that specific environment and plan accordingly. A risk assessment should be undertaken to understand the specific controls, technology and training requirements; users should consult with their security teams for further guidance.

International remote working

18. International remote working is defined as working anywhere outside of the UK away from the user's host country's UK Sovereign Mission.

19. Before undertaking international remote working, users must ensure they have the requisite approvals in place in line with their local organisational HR and security policy. The organisation's SA/SSA should advise on what protective controls are required to manage the specific contextual security risks associated with that location.

Security incidents when remote working

20. All suspected or actual incidents, such as loss of assets, tampering, or compromises of information handled or held remotely, must be immediately reported to the security team in line with organisational policy.

Flexible Remote Working		
OFFICIAL		**SECRET**
Verbal	• Discussions: In public areas be aware of whether you can be overheard by any unauthorised individuals, such as members of the public, or smart listening devices, and avoid discussing classified information in public spaces other than as set out in the Guidance 1.1: Working at OFFICIAL baseline behaviours.	• Discussions: SECRET information must never be discussed in public places or locations where you could be overheard by unauthorised individuals or smart listening devices. Specialist countermeasures can be deployed to enable verbal SECRET discussions in flexible and international remote working locations, but their deployment is subject to a professional security risk assessment and other considerations. You must approach your security team for further advice if you wish to utilise this service.

Hard copy	• Printing: Do not print on any public or personal printer, you can only use corporate systems or devices that have been approved by your organisation. Avoid taking hard copy documents from the office to public spaces other than as set out in the OFFICIAL controls. • Disposal: Documents must not be disposed of in publicly-accessible bins e.g. a hotel room bin. They should be retained securely until they can be disposed of in accordance with the GSCP policy. • Storage: Store OFFICIAL information marked -SENSITIVE under a single barrier and a lock and key (e.g. a lockable cupboard or safe) if leaving them unattended, in order to prevent individuals who can access the workspace from viewing classified material. If that is not possible, the documents must be kept on your person until suitable storage is available.	• Printing: Do not print on any public or personal printer, you can only use corporate systems or devices that have been approved by your organisation for SECRET or higher. Hard copies of SECRET information should not be removed from the workplace, except in exceptional circumstances for remote work. Where it is necessary to work on hard copy SECRET information at a remote working site away from home, there must be prior senior management (at least SCS1 or equivalent) approval in writing. All SECRET documents must be checked out in a Protected Document Registry book. • Disposal: Retain information until you can dispose of information in accordance with the NPSA Secure Destruction Standard with products from the Catalogue of Security Equipment (CSE). • Storage: Do not leave hard copy SECRET information unaccompanied. Keep it on your person at all times.

Electronic	• Access: The need-to-know principle applies when reading OFFICIAL classified information on a laptop, mobile or hardcopy documents. Be aware of the possibility of being overlooked and do not allow unauthorised individuals, such as members of the public, to do so. Avoid accessing classified information in public spaces other than as set out in the OFFICIAL controls. When setting a password, you should use the 'three random words' strategy set out by NCSC's guidance and these should be kept securely away from the device.	• Access: Do not leave SECRET accredited laptops or mobiles unaccompanied. When away from a SECRET laptop, even for a short time, always remove any token or CIK and keep discreetly in your possession separately from the device. SECRET accredited laptops and mobile devices must be kept in your possession or held discreetly in approved tamper evident containers, ideally in physical security equipment / furniture provided by your organisation. Do not write down passwords.