Cabinet Office

Government Security Classifications Policy Quick Read

30 June 2023

The Government Security Classifications Policy (GSCP) sets out the administrative system used by HM Government (HMG) to protect information and data assets appropriately against prevalent threats through the use of 'classification tiers'.

Overview

1. This Quick Read provides a short overview covering a:
    a. summary
    b. definitions for OFFICIAL, SECRET and TOP SECRET;
    c. baseline security behaviours for the three classification tiers;
    d. standardised additional markings (including: handling instructions, descriptors, prefixes and national caveats); and
    e. guidance for remote working.

Summary

2. HMG uses three classification tiers (OFFICIAL, SECRET and TOP SECRET). Each tier provides a set of recommended baseline behaviours and a set of protective controls, which are proportionate to the threat profile for that tier AND the potential impact of a compromise, accidental loss or incorrect disclosure of information held within that tier.

3. All information that is created, processed or moved (sent and received) by, within, or on behalf of HMG falls within the GSCP and must be protected in a manner consistent with the baselines for each classification tier. This is because all information that HMG needs to collect, store, process, generate, dispose or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

4. In addition to the GSCP baseline behaviours and security controls, information MUST be protected in accordance with all relevant legislative or regulatory requirements, including any international agreements and obligations.

5. The GSCP baselines must be met regardless of where the information is collected, stored, processed or shared across HMG and with the wider public sector and external partners. This consistency is essential to provide the confidence that underpins effective information sharing and interoperability between organisations. Organisations may apply additional controls in line with the organisation's risk appetite above the baselines outlined in the GSCP, but not below. Access to information must ONLY be granted where there is assurance that appropriate security controls (personnel, physical, procedural and technical) are in place.

6. The handling and distribution of information covered by the GSCP needs to balance two principles: need-to-know and need-to-share. The outcome should be that access to information (regardless of classification) is restricted to those who need to know, which will normally include those appropriately cleared and who require the information to be effective in their role. The size of the group who has access to classified information can be small or large, but information sharing must meet the minimum security controls for the relevant classification.

7. Everyone who works in or with the government (including staff, contractors and service providers) has a duty of confidentiality coupled with a responsibility to safeguard any HMG information or data that they access and/or share (irrespective of whether it is marked or not), and they must be provided with appropriate training. Individuals are accountable for their own security decisions.

8. All HMG information should, where possible, be clearly marked with a classification tier. Local organisational policy set by a Security Advisor/Senior Security Advisor or Head of Security may override this requirement for OFFICIAL information only on the basis of business need. In this case, information is deemed to be OFFICIAL in the absence of any other marking.

9. There is additional guidance for Security Advisors/Senior Security Advisors and Heads of Security on their obligations in Guidance 1.5: Considerations for Security Advisors. SAs/SSAs should read the policy in full before setting local organisational policy.

Definitions

10. The updated definitions for the classification tiers are set out below (threat profiles and risks of compromise can be found in the full policy).

a. **OFFICIAL:** 'The majority of information that is created, processed, sent or received in the public sector and by partner organisations, which could cause no more than moderate damage if compromised and must be defended against a broad range of threat actors with differing capabilities using nuanced protective controls.' OFFICIAL-SENSITIVE is not a separate classification tier. Further information about this additional marking is found below.

b. **SECRET:** 'Very sensitive information that requires enhanced protective controls, including the use of secure networks on secured dedicated physical infrastructure and appropriately defined and implemented boundary security controls, suitable to defend against highly capable and determined threat actors, whereby a compromise could threaten life (an individual or group), seriously damage the UK's security and/or international relations, its financial security/stability or impede its ability to investigate serious and organised crime.'

c. **TOP SECRET:** 'Exceptionally sensitive information assets that directly support or inform the national security of the UK or its allies AND require an extremely high assurance of protection from all threats with the use of secure networks on highly secured dedicated physical infrastructure, and robustly defined and implemented boundary security controls'.

Baseline Security Behaviours

11. The GSCP outlines the minimum baseline security behaviours users should follow at each classification tier. It covers the baseline behaviours at each tier for the handling (sharing, storage, transport, and destruction) of information in electronic, hard-copy and verbal formats. These baseline behaviours provide protection proportionate to the level of risk.

12. Each set of baseline behaviours that users need to follow can be found in:

    a. Guidance 1.1: Working at OFFICIAL;

    b. Guidance 1.2: Working at SECRET; and

    c. Guidance 1.3: Working at TOP SECRET.

13. Users should ensure they are familiar with both the GSCP and local security guidance before handling classified information.

Using Additional Markings

14. The GSCP 2023 introduces a non-exhaustive standard list of additional markings (handling instructions, descriptors, prefixes and national caveats). HMG organisations may define further additional markings and users should ensure they are familiar with any locally-defined markings.

15. The GSCP 2023 also contains guidance on when the -SENSITIVE marking should be applied to OFFICIAL information (this can be found in Guidance 1.1: Working at OFFICIAL).

16. In short, the -SENSITIVE marking should be applied to OFFICIAL information that is not intended for public release and that is of at least some interest to threat actors (internal or external), activists or the media. A compromise of OFFICIAL information or material marked -SENSITIVE is likely to cause moderate damage to the work or reputation of the organisation and/or HMG and must be marked with the -SENSITIVE marking. Such information must be handled using the additional marking and with other additional controls

17. Additional markings should be applied in conjunction with a classification to: indicate the nature or source of the information; limit access to specific user groups; and, indicate whether additional protective controls are required to protect the information. Not all additional markings can be used with every classification. Below is a table showing which Handling Instructions and Descriptors can be used at each classification tier:

Handling Instructions	OFFICIAL	SECRET	TOP SECRET		OFFICIAL (with –SENSITIVE marking)
RECIPIENTS ONLY	YES	YES	YES		YES
FOR PUBLIC RELEASE	YES	NO	NO		NO
ORGANISATION USE ONLY	YES	YES	YES		YES
HMG USE ONLY	YES	YES	NO		YES

EMBARGOED	YES	YES	NO		YES
Descriptors					
LEGAL PROFESSIONAL PRIVILEGE (LPP)	YES	YES	YES		YES
LEGAL	YES	NO	NO		YES
MARKET SENSITIVE	YES	YES	YES		YES
COMMERCIAL	YES	YES	YES		YES
HR MANAGEMENT	YES	NO	NO		YES
PERSONAL DATA	YES	NO	NO		YES

Remote Working Guidance

18. The GSCP 2023 contains updated guidance on how to handle classified information whilst working remotely at OFFICIAL and SECRET. Remote working is where users work for any length of time in a location other than their organisation's principal site in the UK. Remote working has become more common 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.

19. When working remotely, users must protect information to the same standard as working in the office, if not a higher standard to manage these additional risks. There are some key considerations included in the policy for all 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.

    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.

20. The policy covers in further detail the security controls for working remotely at their home, flexible remote working and internationally, see Guidance 1.5: Working Remotely at OFFICIAL and SECRET.