Cabinet Office

Procurement Policy Note: Government Security Classifications Policy 2023

Action Note 07/23 June 2023

Issue

1. The Government Security Classifications Policy (GSCP) has been updated to address gaps in the previous policy and changes in government working practices since the last major update in 2013. The Policy applies to any information or data that is created, processed, stored or managed as part of an HMG contract.

Dissemination and Scope

2. The contents of this Procurement Policy Note (PPN) apply to all Central Government Departments, their Executive Agencies, Non-Departmental Public Bodies and NHS bodies. These organisations are referred to in this PPN as 'In-Scope Organisations'.

3. Please circulate this PPN within your organisation, particularly to those with a commercial, procurement and/or contract management role. The GSCP should also be shared with your information assurance and data protection leads.

4. Other public sector contracting authorities creating, processing, storing or managing data or information as part of an HMG contract may wish to apply the approach set out in this PPN.

Timing

5. The contents of this PPN should be implemented by June 2024. This 12-month implementation window is to allow sufficient time for the requirements of the updated classifications policy to be integrated into commercial activity.

Action

6. In-Scope Organisations must ensure that appropriate protective security controls are in place for new and existing contracts in line with the updated GSCP. A full suite of guidance documents is available on GOV.UK, with specific guidance for commercial teams and suppliers set out in ***Guidance 1.6: Contractors and Contracting Authorities*.**

7. The majority of these updates are minor changes which will not require a contract variation to existing contracts. However, there might be some instances where specific contracts need to be reviewed.

8. In-Scope Organisations should notify existing suppliers that the GSCP has been updated and set out any changes needed to the contract.

9. In-scope Organisations should familiarise themselves with the following aspects of the updated GSCP:

a. Updated definitions for the three classification tiers OFFICIAL, SECRET and TOP SECRET.

b. Baseline security behaviours for the three classification tiers and further security controls for when the -SENSITIVE marking is applied to OFFICIAL information. OFFICIAL-SENSITIVE has not been introduced as a new classification tier.

c. Updated list of principles to be followed by anyone handling HMG information.

d. Standardised additional markings (including: handling instructions, descriptors, prefixes and national caveats).

e. New guidance for remote working when handling HMG information,

f. Updated guidance on aggregation and further considerations.

10. All HMG information should, where possible, be clearly marked with a classification tier.

Training

11. As the GSCP applies to the whole of an organisation, departmental Security Advisors will be in receipt of education and awareness materials entitled 'Mark My Words' (obtained via the Security Education and Awareness Centre hosted within DWP). This includes an information video which can be sent to suppliers.

12. A new E-Learning module is also available on the Government Campus entitled 'Security Classifications'.

Background

13. 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'.

14. 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.

Contact

15. Enquiries about this PPN should be directed to the Helpdesk (telephone 0345 410 2222, email info@crowncommercial.gov.uk).

16. Enquiries regarding the application of the policy should be sent to the Government Security Function at gsfinfo@cabinetoffice.gov.uk.

Cabinet Office

Annex A - Definitions and Additional Markings

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

- **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.
- **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.'
- **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

2. 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.

3. 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.

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

Using Additional Markings

5. 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.

6. 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).

7. 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

8. 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