Cabinet Office

Government Security Classifications

FAQ Sheet 1: Working with OFFICIAL Information

v1.2 – April 2013

This FAQ sheet addresses practical aspects of working with the OFFICIAL level of the Government Security Classifications Policy (December 2012). It is intended to help information owners and transition planning teams to understand the new policy, and to support consistent approaches to implementation that can ensure trust, interoperability and effective sharing.

GENERAL PRINCIPLES

1. The public sector holds a very wide range of information and delivers many different services, but many of the information risks organisations must manage are broadly similar. The majority of information related to public sector business, operations and services can be managed as OFFICIAL. Indeed most organisations will operate almost exclusively at this level.
2. There is no unclassified level below this - any information that is created, processed, generated, stored or shared within (or on behalf of) HMG is OFFICIAL by definition.
3. There is no requirement to mark routine OFFICIAL information.
4. Personnel, physical and information security controls for OFFICIAL are based on commercial good practice, with an emphasis on staff to respect the confidentiality of all information. In some instances a more limited need to know must be enforced and assured. A single handling caveat '**OFFICIAL-SENSITIVE**' provides for this.
5. **OFFICIAL–SENSITIVE** must be clearly marked.
6. Three optional descriptors may be used (in conjunction with a security classification) to distinguish specific types of information in the following circumstances – note that descriptors do not attract additional security controls per se:
    a. To limit circulation of sensitive information that locally engaged staff overseas cannot access;
    b. To distinguish commercial or market sensitive data, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed;
    c. To identify particularly sensitive information relating to an individual (or group), where inappropriate access could have damaging consequences.
7. The use of descriptors is at an organisation's discretion. But where they have been applied by an originator, they should be carried forward.

USING THE NEW MARKINGS:

How does the OFFICIAL classification map to the existing Government Protective Marking System (GPMS)?

There is no direct correlation between the new classification policy and the old GPMS scheme. In general terms, assets that were previously classified up to and including RESTRICTED should be managed at OFFICIAL. Although the review found instances where some information was over marked at CONFIDENTIAL and this may be appropriate to manage as OFFICIAL too. Originators need to think about the nature and context of any information they handle when deciding whether it is appropriate to particularly enforce need to know through use of the OFFICIAL-SENSITIVE caveat.

There is a materially different threshold for SECRET assets, both in terms of threat and the impact of compromise. RESTRICTED (or CONFIDENTIAL) information should only move into the SECRET tier if the organisation's SIRO has assured themselves that BOTH the consequences of compromise or loss correspond to the impact statements set out in the classification policy; AND that the information needs to be defended against highly capable, determined and well resourced threat actors as described in the SECRET threat profile (in essence hostile foreign intelligence services or high-end organised crime groups).

The Threat Profile for OFFICIAL does not include highly capable, determined and well resourced organised crime groups and state actors. Should (formerly) RESTRICTED information be moved into the SECRET tier?

Asset owners need to consider the sensitivity and threats to their information. In most cases, formerly RESTRICTED should be managed as OFFICIAL with appropriate procedural controls to enforce need to know restrictions. Whilst the controls at OFFICIAL (e.g. 'good' commercial ICT products and services) cannot absolutely assure against the most sophisticated threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access this information. In this respect it is no different from current arrangements for the lower classification levels.

Organisations must be mindful that there is a very significant step-up (a cliff face) from OFFICIAL to SECRET, and that the benefits of the new policy will be eroded if they are too risk averse and seek to put more information into SECRET then is absolutely necessary.

Will information in the OFFICIAL level be widely accessible?

No. There is no presumption of disclosure or unbounded access at any level of the classification policy; though the principles of openness, transparency and information reuse require that individuals to consider the proactive publishing of information and data sets where appropriate.

As with current arrangements, organisations should use proportionate ICT access controls, supported by procedural and personnel controls, to manage their information assets and enforce need to know restrictions.

Is there an unclassified tier below OFFICIAL?

No, the new classification system has quite purposefully taken UNCLASSIFIED out of the equation. ALL information that is created, collected, processed, stored or shared within government (and across the wider Public Sector) has value, belongs to the organisation and must be handled with due care. This includes published data where integrity and availability considerations (and often Crown Copyright) may continue to apply.

In keeping with the overall Civil Service Reform Plan, the ethos is to move away from process driven approaches that seek to do all the thinking for people. Individuals are expected to think abut the nature and context of the information they work with and to exercise good judgement to ensure that HMG information (and other assets) is handled and safeguarded appropriately.

Many staff will use publically available information in their work (e.g. raw data from the internet). However, there is no requirement for an 'unclassified' infrastructure to manage this information as anything that staff create or process is by definition OFFICIAL.

What is the threshold for using the caveat OFFICIAL-SENSITIVE?

Organisations and staff should use their discretion to determine those instances where it will be appropriate to use the OFFICIAL-SENSITIVE caveat as this will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements. Organisations need to make their own judgements about the value and sensitivity of the information that they manage, in line with departmental and HMG corporate risk appetite decisions.

However, the handling caveat should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for HMG more generally. This might include, but is not limited to the following types of information:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to ministers on contentious and very sensitive issues;
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- more sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but does not require SECRET-level protections;
- diplomatic activities or negotiating positions where inappropriate access could impact foreign relations or negotiating positions and must be limited to bounded groups;
- very sensitive personal data, where it is not considered necessary to manage this information in the SECRET tier.

In all cases, individuals need to be trained to understand the sensitivities related to the information they work with (including any statutory or regulatory requirements), supported by local business processes, and instructed about the need to provide meaningful guidance when sharing that information with others.

Does OFFICIAL-SENSITIVE have to be registered and tracked?

There is no blanket requirement to register (and track) OFFICIAL-SENSITIVE information assets, though in some cases the consequences of loss or inappropriate access to individual information assets may be particularly damaging (e.g. export licensing, witness data, information of use to terrorist / extremist targeting etc). Organisations need to make their own judgements about the value and sensitivity of the information that they process and whether additional procedural safeguards may be appropriate to manage the associated risks. Where large volumes of OFFICIAL-SENSITIVE information about particular topics are regularly shared between organisations, the respective SIROs and IAOs may wish to agree specific handling arrangements and transfer protocols in line with the policy.

Can organisations use additional markings to indicate particular types of information?

In support of information handling arrangements, departments may find it helpful to use a descriptor to identify particular types of OFFICIAL-SENSITIVE information, i.e. where it is locally sensitive (overseas context), commercial- or market-sensitive, or where inappropriate access could be particularly damaging to an individual (or group). These descriptors will not drive any additional security controls per se, but can help to narrow circulations or compartmentalise information.

These are the only descriptors provided for in the policy and departments are discouraged from applying others that might inadvertently complicate or artificially segment the OFFICIAL tier, or detract from the fundamental behavioural change the policy seeks to drive. Such use could lead to unintended and damaging consequences if used in lieu of more meaningful handling advice, either by inhibiting information exchanges or, conversely, by allowing for unnecessarily wide circulations.

Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate. Rather than using generic labels, staff should offer meaningful handling advice where appropriate, that describes any particular sensitivities. For example, by writing at the top of an email: *"attached a draft submission that seeks final Ministerial clearance for [insert]. This is for your eyes only – it remains highly contentious and should not be copied any further."*

How should organisations enforce security breach policies?

Organisations must ensure that their staff are properly trained to understand that they have a duty of confidentiality and a personal responsibility to safeguard any HMG information that they are entrusted with. This includes clearly explaining the potential sanctions (criminal or disciplinary) for inappropriate behaviours. Training should be supported by common sense local business processes that make it easier for staff to follow the rules (e.g. clear desk policies, separating non-HMG printed research from OFFICIAL papers, guidance on proper

disposal etc). There is also an expectation on managers to ensure that their staff understand and comply with their personal responsibilities.

Where inappropriate behaviours or security breaches are apparent they should be dealt with on a case by case basis - the likely consequences of compromise or loss will vary significantly for different types of OFFICIAL information and in some cases may constitute a criminal offence. HR policies and procedures should complement security policies and any disciplinary sanctions should be applied in a measured and proportionate way.

How should personal data be managed? Do the Data Handling Review (DHR) requirements still apply?

Handling personal data within the new classifications is covered separately in *FAQ Sheet 2: Working with Personal Information*.

How should UK information that is sent overseas be marked?

Detailed guidance on the equivalencies between UK and international classification systems, and any supplementary handling or protection requirements, is provided in separate guidance. In general terms, any sensitive HMG information that is shared with international partners must be marked with the 'UK' prefix to identify the originator and provide a measure of protection under partners' freedom of information legislation.

How should time-sensitive information be managed?

Individuals should be encouraged to provide meaningful guidance on handling any sensitive information that they share, including if sensitivities are time-bound and information can be distributed more widely after a particular date or event, e.g. in the case of official statics or the Budget. The Classification Policy does not mandate a format for such guidance.

Who can mark / unmark a document?

The originator is responsible for determining the appropriate classification for any assets they create, though recipients / holders of copies may challenge the classification with a reasoned argument if necessary. Depending on context and circumstances sensitivities may change over time and it may become appropriate to reclassify an asset.

Every effort should be made to consult the originator or originating organisation before a sensitive asset is considered for disclosure, including release under FOIA or to the National Archives. Where the originating organisation cannot be identified (e.g. following Machinery of Government changes) it is good practice to consult with copy recipients.

Where an asset is originated by a foreign government or international organisation, the originator must always be consulted before the asset can be remarked or disclosed to an individual that does not hold the appropriate personnel security control.

When should organisations start to apply the new markings?

Central government, the Armed Forces and external partners should begin to apply the new classification markings from go live in April 2014. Go live will be using existing ICT and under existing commercial arrangements with transition to the new technical standards and contractual conditions (defined by the Government Procurement Service) in line with scheduled business cycles.

Does existing information need to be remarked?

No. As a rule, organisations are not required to retrospectively remark legacy information or data that uses the old protective markings. Nor does information or data need to be remarked where it is in continued use within an organisation, provided that users / recipients understand how it is to be handled in line with the new Classification Policy.

However, where legacy information or data bearing a former protective marking is to be shared or exchanged between organisations, or with external partners, the originator should consider remarking with the appropriate security classification. At the very least, meaningful guidance should be provided about how the asset should be protected in line with the new approach.

Further information about procurement, contract variation and classified contracting will be provided separately.

Who in my own organisation can I go to for advice on valuing my assets?

The information assets within your organization are the responsibility of Information Asset Owners (IAOs) Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide advice to the SIRO on the security and use of their asset.

Notes:

1. This FAQ sheet will be updated regularly. If an organisation has a request for specific advice on handling OFFICIAL information then please contact the Government Security Secretariat team via the mailbox: gpms@cabinet-office.x.gsi.gov.uk.

2. This FAQ sheet is part of a series, including:

- Briefing for Senior Leaders
- FAQ Sheet 2: Working with Personal Information

Additional FAQ sheets will be developed as implementation progresses.