National Offender Management Service

Government Secure Classification Policy

This instruction applies to :-		Reference :-
NOMS Headquarters Prisons National Probation Service and Community Rehabilitation Companies		**AI 10/2014** **PSI 12/2014** **PI 04/2014**
Issue Date	**Effective Date**	**Expiry Date**
31 March 2014	02 April 2014	01 April 2018
Issued on the authority of	NOMS Agency Board	
For action by	All staff responsible for the development and publication of policy and instructions *(Double click in box, as appropriate)* ☒ NOMS HQ ☒ Public Sector Prisons ☒ Contracted Prisons* ☒ Governors ☒ Heads of Groups ☒ Community Rehabilitation Companies ☒ National Probation Service *And successive organisation within the new NPS and Community Rehabilitation Companies structure* **** If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	Service improvement/Legal compliance	
For information	All staff	
Provide a summary of the policy aim and the reason for its development / revision	The new Government security classification (GSC) scheme is being launched by the cabinet Office across all government departments on 2 April 2014 and across NOMS a series of communications, training and briefing events for staff are underway to support the launch of the new scheme. This policy underpins these events and sets out the mandatory requirements of the new scheme. The scheme will classify the great majority of NOMS information, including the majority of offender records, as OFFICIAL and these will not be protectively marked.	
Contact	NOMS Information, Assurance and Policy Team Tel: 0300 047 6590 - Email: informationassurance@noms.gsi.gov.uk	
Associated documents	PSO 9010 – IT Security PSO 9015 – Information Assurance PSO 9025 - Archiving Retention and Disposal	

Replaces the following documents which are hereby cancelled: This document replaces the guidance on the Government Protective Marking Scheme in PSO 9015 Information Assurance and PI 09/2009 Information Assurance

Audit/monitoring: Compliance with this instruction will be monitored by Internal Audit & Assurance.

Introduces amendments to the following documents: None

CONTENTS

1 Executive Summary

Background

1.1 The Government Security Classification (GSC) system provides a framework for classifying information. Classification directs users to particular levels of control which are required to ensure the continuing availability, integrity and confidentiality of information. The criteria for determining the correct classification have regard to both the level of threat **and** the impact should the information be compromised.

1.2 This policy describes how NOMS classifies information assets to ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation. The policy applies to all the information that NOMS collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with delivery partners and third party suppliers.

1.3 Everyone who works within NOMS has a duty to respect the confidentiality and integrity of any NOMS information and data that they access, and is personally accountable for safeguarding assets in line with this policy.

1.4 NOMS information assets must be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each type requires a minimum set of security controls to be in place which need to be able to provide the appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

1.5 All staff should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners and wider supply chain. Delivery partners and suppliers who have access to NOMS information must apply equivalent controls, which should be provided for under contractual provisions or information sharing agreements.

Desired outcomes

1.6 This policy sets out NOMS commitment to the management of information. It also sets out what prison establishments, National Probation Service, headquarters groups, NOMS 'delivery partners' and third party suppliers should do to manage information. In doing so, this policy supports the NOMS strategic aims and objectives and should enable employees throughout the organisation to identify an acceptable level of risk and, when required, use the handling controls.

Application

1.7 All NOMS staff, contractors, third party suppliers and delivery partners are responsible for ensuring that all information is looked after with care to enable the business to function as well as meeting privacy needs.

Mandatory actions

1.8 *From 2 April 2014 all staff, contractors, third part suppliers or delivery partners must apply the new scheme to any new documents that are produced but they will not be required to apply the new scheme retrospectively.*

1.9 *ALL information that NOMS needs to collect, store, process, generate or share to deliver services and conduct MoJ business has intrinsic value and all staff must apply the appropriate degree of protection.*

1.10 *Everyone who works with NOMS (including staff, contractors, delivery partners and third party suppliers) has a duty of confidentiality and a responsibility to safeguard and NOMS information or data that they access irrespective of whether it is marked or not and must be provided with the appropriate training.*

1.11 *Access to sensitive information must only be granted on the basis of a genuine need to know and an appropriate personnel security control.*

1.12 *Information assets received or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including contracts or information sharing agreements.*

1.13 *Any business area holding or expecting to hold information at SECRET or TOP SECRET must contact the Agency Security Officer to agree handling controls.*

Resource Impact

1.14 All staff are required to complete the Cabinet Office training package provided either by e-learning or PowerPoint by 31 March 2014. Completion of the training should between 10 to 20 minutes per staff member if completed via e-learning.

1.15 All staff joining NOMS after this date will be required to complete the Responsible for Information e-learning course on CSL which includes a module on the new GSC scheme. Completion of the full training package should take between 40 to 50 minutes.

1.16 All forms and templates on ICT systems that currently show the GPMS markings (PROTECT/RESTRICTED/CONFIDENTIAL) must be updated to reflect the new GSC. Information Asset owners are responsible for ensuring the updates take place within the following timescales:

- Local standalone IT or locally networked systems must be updated by 30 September 2014. The resource impact should be minimal as the templates can be amended as and when they are required but this will be depend on the number of forms in use.
- National systems such as P NOMIS / nDelius / OASys must be updated by 30 September 2015, the changes should be factored into planned maintenance upgrades to reduce the cost implications:

1.17 There is a requirement to update existing policies whose contents make reference the old Government Protective Marking Scheme (GPMS) by 30 June 2014.

1.18 There is no requirement to apply this policy retrospectively and so following a period of familiarisation the implementation should be carried out at business as usual.

(Approved for publication)

Ben Booth,
Director of Change and ICT, NOMS

2. The Government Security Classification System

2.1 The new classification system has three levels: OFFICIAL, SECRET and TOP SECRET.

2.2 New GSC classifications indicate the sensitivity of information in terms of the likely impact resulting from compromise, loss or misuse, and the need to defend against a broad profile of applicable threats. There are three new levels of classification:

OFFICIAL

The majority of information that is created / processed by NOMS.

Includes routine business operations, including offender and staff personal information, and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined / highly capability threats.

Where compromise may seriously damage military capabilities, international relations or the investigation of serious organised crime.

TOP SECRET

HMG's most sensitive information requiring the highest levels of protection from the most serious threats.

Where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

2.3 The security classifications do not have any direct implications for access to information under either the Data Protection Act (1998) or the Freedom of Information Act (2000). Further guidance on these two acts can be found in PSO 9020. If information has a marking, this does not mean that it is exempt from being disclosed, and if information does not have a marking, this does not mean that it can be automatically disclosed. The existence of a protective marking might help to make a decision about access, but every case must be considered on its own merits.

2.4 Disciplinary action will be considered for any member of staff (including contractors, consultants, and suppliers so far as is feasible) who do not follow the mandatory actions set out in this policy.

OFFICIAL

2.5 This classification will apply to the vast majority of NOMS information including:

- general NOMS activity (finance, estates, personnel, policy, commercial),
- most front line service operations,
- organisation and performance management information,
- personal information (including staff data, offender case files, citizen data) and
- policy documents.

2.6 The classification reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act and Public Records Acts.

2.7 *The controls in place must be sufficient to protect against a range of impacts and threats*:

- the sorts of threats faced by a major UK company: hacktivists, single issue pressure groups, investigative journalists, competent individual hackers, the majority of criminal individuals or groups.

OFFICIAL information does not require a protective marking

2.8 *A limited amount of information will be particularly sensitive but will still come within OFFICIAL if it is not subject to the threat sources for which SECRET is designed, even if its loss or compromise could have severely damaging consequences. This information can be described as OFFICIAL SENSITIVE and the need to know principle must be rigorously enforced for particularly where it may be being shared outside of a routine or well understood business process.*

2.9 There will be very few activities where all related information or cases require the OFFICIAL SENSITIVE marking, though this may apply to assets previously marked as CONFIDENTIAL. Examples include:

- Where there is a specific risk assessment, or threat to highly vulnerable individuals
- Cases involving intimidation, corruption or fraud
- Where there is a legal requirement for anonymity
- Where there is a high media profile and risk of damaging unauthorised disclosure
- Highly sensitive change proposals or contentious negotiations.
- Major security or contingency planning details

This more sensitive information must be identified by being marked 'OFFICIAL SENSITIVE'. This marking alerts users to the enhanced level of risk and that additional controls are required.

SECRET

2.10 *Use of SECRET must only be used where there is a high impact **and** a sophisticated / determined threat (elements of serious and organised crime and some state actors):*

- Classified material received from OGDs/agencies relating to national security and counter-terrorism
- Intelligence and investigations relating to individuals of interest to security agencies
- Information that could serious damage national security and intelligence operations
- Information affecting the ability to investigate or prosecute serious/organised crime where there is intelligence to suggest there is a known sophisticated and determined threat to access the information.
- Personal/case details where there is a specific threat to the life/liberty of an individual such as protected witness scheme records

2.11 The concept of sophisticated or heightened threat doesn't only apply to those with a high technical (IT) attack capability but can apply to criminals who have a developed capability to intimidate or coerce individuals. i.e. if disclosure of information could result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information must be tightly controlled.

2.12 *SECRET must not become the default status for material just because of the type of case or potentially severe consequences (e.g. murder trials, or where there is a threat to life). The threat capability must also be present.* There is no change to controls at this level.

Any business area holding or expecting to hold information at this level must contact the Departmental Security Officer (DSO) to agree controls.

TOP SECRET

2.13 This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level.

Any business area holding or expecting to hold information at this level must contact the DSO to agree controls.

2.14 Further details on the new markings and on how they should be applied can be found in the Annexes of this policy.

3. Transition to the Government Security Classification System

3.1 *When the new system goes live on 2 April 2014 all staff, contractors, third party suppliers or delivery partners must apply the new scheme to any new documents that are produced but they will not be required to apply the new scheme retrospectively.* This means that staff do not need to go back to all the information assets that have been marked with the previous GPMS (UNCLASSIFIED/PROTECT/RESTRICTED/CLASSIFIED etc) and change them to the new system.

3.2 However, some of this information, such as offender and staff records, will be current and will be used on a regular basis. In this case the old marking will need to be mapped on to the new system. For information bearing the 'old' markings, the guidance in Annex B should be followed to ensure appropriate handling.

3.3 *Unless there are specific instructions to the contrary, staff must maintain the current levels of control and use existing ICT systems on which information is currently held/processed.*

3.4 The old protective markings do not automatically read across, particularly at CONFIDENTIAL however it is likely that:

- all material up to and including RESTRICTED will become OFFICIAL.
- Much material at CONFIDENTIAL will become OFFICIAL but some may become SECRET.
- Only a limited amount of material at RESTRICTED will need marking as OFFICIAL-SENSITIVE.
- CONFIDENTIAL material moving into OFFICIAL is likely to require marking as OFFICIAL SENSITIVE.

Additional guidance about mapping to the new system can be found in Annex B

4. How to Handle Information in the GSC System

4.1 At OFFICIAL any local instructions or operating procedures that are in place will continue to be followed and these should assist all staff in identifying any cases that require the OFFICIAL SENSITIVE marking.

4.2 The flow chart at Annex E can be used if you are concerned that information requires additional security controls and believe that the information may marking OFFICIAL SENSITIVE.

4.3 Further detailed information such as the controls framework and examples of the type of information that would fall into OFFICIAL can be found in the Annexes to this policy and provide some general rules. You can also refer to the IPA GSC intranet pages where you can find desk-aids entitled 'Working with Official information', posters and FAQs which will help you if you are creating or processing any non-routine material.

4.4 *Business areas/Information Asset Owners must review risks to their information and ensure local procedures are in place, adopting additional controls where needed*.

4.5 The Security Controls Framework at Annex D identifies additional considerations under some aspects of control. Business areas/IAOs may decide to adopt more robust controls in these areas, particularly for material marked OFFICIAL SENSITIVE or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

4.6 *Controls must be applied proportionately for information which would previously have been unclassified.* Such information will still need looking after if it is needed to do the job, but must not be marked as UNCLASSIFIED and may not require controls designed to provide confidentiality.

4.7 *If IAOs or staff are considering classifying any new assets or reclassifying any existing assets as SECRET or TOP SECRET, they must consult the IPA Team at informationassurance@noms.gsi.gov.uk or on 0300 047 6590 or the DSO in Security Policy Group to determine whether a heightened threat might be present, and to agree necessary controls.*

5. Applying the appropriate GSC controls to personal information

5.1 In most cases (apart from where other particular sensitivity considerations apply) personal information and sensitive data, as defined by the Data Protection Act (DPA), will be handled within OFFICIAL without any caveat or descriptor. Security Classifications are designed to be used in parallel with any DPA controls but will not in themselves provide the requisite protection for information covered by DPA.

5.2 *All personal information must be subject to appropriate protection. There is no presumption of uncontrolled access to information at any level of the classification policy; though the principles of openness, transparency and information reuse need to be considered. As with current arrangements, staff must use ICT access control measures provided by the secure email (for example GSI / PSN or CJSM), supported by procedural and personnel controls, to manage personal information assets and enforce the "need to know" principle.*

5.3 All personal data / information is subject to the "need to know" principle and it is the responsibility of individuals to ensure that this is enforced in respect of personal data / information for which they are responsible.

5.4 *Everyone working with NOMS information, staff, contractors third party suppliers and delivery partners, has a personal responsibility to safeguard any personal information or data that they access, irrespective of whether it is marked or not.*

When to use the OFFICIAL SENSITIVE caveat for personal information

5.5 *The OFFICIAL-SENSITIVE caveat must be applied where the "need to know" must be most rigorously enforced, particularly where information may be being shared outside of a routine or well understood business process.* For example, where the loss or compromise of information could have severely damaging consequences for an individual or group of individuals - there is a clear and justifiable requirement to reinforce the "need to know" principle particularly rigorously across the organisation. Examples may include but are not limited to:

- VISOR data
- Sensitive personal information relating to potential staff corruption
- Personal information forming part of sensitive or high profile investigations
- CHIS / RIPA documentation
- Personal data of high profile offenders or victims

5.6 *To maintain its currency the threshold for marking information OFFICIAL-SENSITIVE must be kept quite high.* It is certainly not intended that because an OFFICIAL document or data contains personal information it should be routinely marked OFFICIAL-SENSITIVE, it must meet the criteria set out above.

Transmitting Personal Information

5.7 Current rules continue to apply when sending OFFICAL documents containing personal information across the Internet. Personal information may be sent over secure government email systems such as the GSI/PSN or CJSM or in encrypted / password protected documents across the Internet. However there are circumstances where it may be appropriate to send unencrypted personal data over the Internet. *Before unencrypted personal information is sent across unsecured networks a risk assessment must be undertaken to assess the consequences of compromise.*

5.8 *This assessment must also consider the operational or valid business reasons for this requirement, for example an individual has given permission for their information to be sent via the Internet in order to access or receive a service.*

5.9 *Aggregated datasets of personal information must never be sent unprotected across unsecured networks*.

5.10 All staff have a duty of confidentiality and a personal responsibility to safeguard any NOMS information that they are entrusted with. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media.

6. Applying Handling Instructions to Documents within the GSC System

6.1 For information that requires additional controls to support the "need to know" principal handling instructions should be used to identify why special handling is required; who is to be allowed access to the information; how that information or data is allowed (or not) to be circulated or forwarded on and how it is to be stored.

6.2 You control how the information you create is to be handled: you can describe any particular sensitivities of the information and offer meaningful handling advice. Additional handling instructions should be included following advice from the Information Asset Owner to identify handling requirements.

6.3 Handling instructions should be included:

- On the front page of any document, and at the top of each page.
- As the first paragraph of any letter or minute.
- As the first paragraph of any email.
- Highlighted in the operations instructions for any dataset.

6.4 Basic formula for handling instructions:

- Reason this is classified as it is
- What you are allowed to do with this information
- What you need to do to ensure it is kept secure

6.5 Example handling instructions:

- "To be opened by addressee only" – for use when sending staff personal information through the post.
- "Please do not distribute this document further."
- "Please do not print and display this document in a public area or where offenders would have sight of the contents"
- "Please do not circulate wider than copy list"
- "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."
- "This information has been produced by NOMS. Do not share outside of NOMS without the written approval of the sender."

7. Marking Information within the GSC System

7.1 *Information assessed as OFFICIAL must not be marked with the security classification*

7.2 *Marking must be applied to information assessed as OFFICIAL SENSITIVE, SECRET or TOP SECRET.*

7.3 Classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This could mean:

- Marking the top and bottom of documents, clearly, in CAPITALS, and CENTRED (in the header and footer)
- Showing the marking in the subject line of emails:
  - type OFFICIAL-SENSITIVE at the start of the subject line, in CAPITALS
  - remember to consider whether material that is sensitive needs to be sent and whether it is safe or appropriate to send if the recipient is outside GSI/PSN
  - you must not email anything at SECRET or above
- Marking the front of folders or binders
  - Apply clearly in a prominent position in CAPITALS
  - Apply the highest classification of any of the contents

<u>Applying GSC to Forms / Templates on ICT Systems</u>

7.4 *All forms and templates on ICT systems that currently show the GPMS markings (UNCLASSIFIED/PROTECT/RESTRICTED/CONFIDENTIAL) must be updated to reflect the new GSC.*

7.5 Information Asset owners are responsible for ensuring the updates take place within the following timescales:

- Local standalone IT or locally networked systems must be updated by 1 April 2015
- National systems such as QUANTUM / OMNI / NICS must be updated by 30 September 2015
- SSC will update all templates and forms on My Services

8. Arrangements for Re-classification of information within the GSC

8.1 Levels of protective marking may alter with time. Some levels will certainly change. For example, a Category A movement order would be classed as sensitive before the event, but not necessarily once the escort or bed watch has been completed. In this example it would be prudent to mark the document “OFFICIAL SENSITIVE until completion of escort”. All marked documents should be reviewed periodically and, when it becomes appropriate, they should be downgraded to the appropriate level. *Documents received from other government departments must not be downgraded without the approval of the originating department or, if this is no longer extant, the Department which has assumed responsibility for the subject.*

8.2 When re-grading a document, any previous protective marking should be deleted in ink and, where appropriate, the new one stamped on the document together with a reference to any documentary authority for it. The amendment should be signed and dated by the member of staff responsible.

9. Reporting Data loss

9.1 Where legislation and regulation requires us to appropriately handle and protect information, those same demands also requires us to report, manage, and in some cases escalate, all events where information requiring protections is either lost or compromised.

9.2 Lost is defined as information that either we do not know its location (this can be both internally and externally) or where we suspect its location and is out of our control. An example of this is a loss through post, where the package is likely with the mail carrier but we have no control over locating it.

Compromise is defined as information that has been subject to unauthorised access, use, or modification.

9.3 A loss or compromise of information could take many forms and could be discovered in different ways. The list below is not exhaustive but examples include:

- loss of an offender file, or one found where it should not be
- information missing in the post or after a fax transmission
- loss of a computer or memory stick
- loss of a mobile phone or Blackberry
- leaving a computer disc or laptop on a train or in any non-secure environment.

Incident reporting requirement

9.4 *Every staff member, irrespective of role, grade, or location, is required to report an event involving loss or compromise of data.*

9.5 Any events of information loss or compromise must be reported to the IPA team at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590 in accordance with the process described in The Information Assurance Policy.

Annex A

Applying the Government Security Classification system

The following considerations apply:

1. All Staff, Contractors, third party suppliers and delivery partners are responsible for ensuring that all information is looked after with care to enable the business to function as well as meeting privacy needs

2. The majority of NOMS, The MoJ and wider government information will fall into the OFFICIAL tier; there is a significant step up to SECRET and TOP SECRET which are essential for national security and the very highest threat areas

3. OFFICIAL provides for a general and sufficient level of control of information (including for ICT systems running applications holding such information, for example P NOMIS, OASys and nDELIUS) which is not subject to heightened threat sources. Within this there is flexibility to apply additional operational controls to reflect sensitivity, for example the controls surrounding access to the MERCURY and VISOR systems.

4. In most areas of NOMS activity will be at OFFICIAL and staff must continue to follow existing business instructions and procedures for handling information that apply to those activities. Such instructions must include provisions for identifying and dealing with more sensitive cases.

5. The Security Controls Framework and the flow chart at Annexes D and E should be referred to when receiving, handling or creating information in any format, which is not routine or covered by general processes/instructions.

6. Material at OFFICIAL will not require a marking to be applied, but must be protected in accordance with the control framework and any local instructions. However, information assessed to be particularly sensitive must be marked OFFICIAL SENSITIVE, giving a clear warning that strict control of access and special handling apply (see below).

7. Staff are expected to comply with local instructions and minimum controls but need to exercise common sense when applying a control isn't possible or would seriously hinder effective business or safety. In all but the most urgent cases, seek approval from your manager or the Information Asset Owner (this will be the governor in a prison, head of group in HQ or Deputy Director in NPS) before adopting lesser controls. Decisions must be risk based and the assessment must be recorded at the earliest convenient opportunity.

8. Existing material with former protective markings (ie UNCLASSIFIED, PROTECT, RESTRICTED) does not need to be retrospectively reclassified (see transition note at Annex B). Templates on central ICT systems will be updated within 18 months and templates on local systems must be updated within 12 months of the 2nd April launch date.

9. Descriptors, such as 'PERSONAL' or 'COMMERCIAL' must no longer be used, though in exceptional circumstances authors may include 'handling instructions' in a document or email to draw attention to particular requirements. Examples of appropriate 'handling instructions' and guidance on when to apply them can be found in Para 7.

Annex B

Transition to the New Classification System

For information bearing the 'old' markings, the following guidance should be followed to ensure appropriate handling. Unless there are specific instructions to the contrary, staff will be expected to maintain current levels of control and use existing IT systems on which information is currently held/processed.

Old marking	New Classification	Examples
UNCLASSIFIED/ NOT PROTECTIVELY MARKED	Treat as **OFFICIAL** (unmarked) Where controls prevent otherwise safe sharing of non-sensitive information IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences (e.g. for the security of IT assets and GSI/PSN code of connection).	▪ Public notices and leaflets ▪ Published information ▪ Information that doesn't contain personal data or other sensitive content ▪ Training materials
PROTECT:	If information relates to general administration, treat as **OFFICIAL** (unmarked). Where used for personal data, maintain existing handling controls. Unless a risk assessment has identified the requirement for additional security controls personal data will be treated as OFFICIAL Individual offender case records assessed as containing particularly sensitive content will need to be marked OFFICIAL SENSITIVE, though these instances may already have been marked RESTRICTED or CONFIDENTIAL.	▪ Documents containing personal data: personnel records, offender case records/files, victim data ▪ General administration not intended for publication
RESTRICTED:	If it relates to general administration there should be a presumption that it can be treated as **OFFICIAL** (unmarked).	▪ General administration ▪ Policy documents ▪ Commercial documents
	Where used for personal data, maintain existing handling controls. Unless a risk assessment has identified the requirement for additional security controls data will be treated as **OFFICIAL** Individual offender case records containing particularly sensitive content will need to be marked OFFICIAL SENSITIVE, though these instances may already have been marked CONFIDENTIAL. You need to consider whether the subject matter is particularly sensitive and there is a need to restrict access, in which case material may additionally require handling/marking as '**OFFICIAL - SENSITIVE**'. Anything with this level of sensitivity may already have agreed handling constraints. If in doubt, discuss with the Information Asset Owner.	▪ The majority of documents containing personal data: offender case records/files, victim data ▪ Particularly sensitive case records ▪ Contentious policy drafts and advice ▪ Sensitive negotiations

CONFIDENTIAL:	a) **hard copy** previously received from another Department: the presumption should be to treat as **OFFICIAL-SENSITIVE** unless there is a clear national security aspect or it relates to protected witnesses (in which case treat as **SECRET**). If you want to reproduce content in an electronic document, check classification with the author/originating Department. b) **electronic copy** received by x-gsi or held on stand-alone system used for CONFIDENTIAL: continue to observe the operating instructions for the system you are using; continue to use x-gsi for any reply and use the marking applied by the original author. Otherwise adopt controls for **OFFICIAL-SENSITIVE**. Note: Electronic records marked CONFIDENTIAL should not be saved on MoJ's existing standard networks (Quantum, NICS, OMNI) or electronic document management systems (HERM) unless/until the originator/Information Asset Owner has issued revised guidance allowing the information to be handled at OFFICIAL (including Official-Sensitive), and the system has been rated to hold material at OFFICIAL (with any additional access controls) – or the system reclassified as SECRET.	▪ Documents relating to corruption or intimidation ▪ Documents relating to intelligence sources ▪ VISOR records ▪ Documents relating to high profile offenders or victims ▪ Documents relating to counter terrorism prisoners
SECRET:	Continue to treat as **SECRET**, subject to any formal review of the classification of the information assets involved in the particular area of activity: a) if hard copy: treat as **SECRET** and log, store, move and dispose of accordingly b) if held on stand-alone system currently rated at SECRET: treat as **SECRET** and observe operating controls for the system.	▪ Material relating to national security or counter-terrorism ▪ Material relating to Protected Witnesses

Annex C

Examples of Official Information

- Personnel records and associated correspondence
- Procurement tenders/contracts and correspondence
- Personal information concerning an individual, including personnel records, offender records, reports, personal development plans, sick leave records, fingerprints, blood samples for pathology.
- Recruitment data, including application forms, board assessments, reports and feedback forms.
- Health and Safety data, including workplace assessments, reports and personal risk assessments.
- Financial data, including local budget information and staff payroll.
- Programme & Project management – project/programme board minutes, briefing, plans, quality reviews, business cases, strategy, etc.
- Constitutional information, including honours and appointments.
- Any minutes, reports or assessments containing sensitive, non-national security matters.
- Offender / prisoner case information
- Sensitive policy development and advice to Ministers
- Bulk Staff, Personnel and Pay records
- Contracts and Procurement
- Finance/ Commercial Information
- Contingency Plans
- Operational information including Information about NOMS ICT systems
- Security Information Reports containing sensitive information

Examples of information that may require the additional controls provided by Official Sensitive

- Documents relating to corruption or intimidation
- Documents relating to intelligence sources
- VISOR records
- Documents relating to high profile offenders or victims
- Documents relating to counter terrorism prisoners

or where significant operational disruption or reputational harm might arise from disclosure

- sensitive corporate and organisational information including significant organisational change proposals prior to consultation
- contentious negotiations
- major security or contingency planning issues
- policy development and advice to ministers on contentious and very sensitive issues (eg prison closures)
- commercial or market sensitive information that may be particularly damaging to HMG or a commercial partner if improperly accessed

Annex D

Government Security Classification system
Security Controls framework

1. This Annex describes typical personnel, physical and information security controls required when working with NOMS assets. It should be read in conjunction with the guidance in this policy document.

2. The identified controls are cumulative - minimum measures for each classification provide the baseline for higher levels.

3. For most business processes, local procedures or instructions should already be in place, which should be consistent with this framework and which will cover the majority of information handling. Staff may need to refer to this framework if handling or creating non-routine material.

4. Some business groups may need to apply controls above (or below) the baseline to manage specific risks to particular types of information. Such exceptions must be agreed by business areas/Information Asset Owners and with delivery partners.

The table below describes standard control measures for the three levels within the security classifications scheme but business areas can adopt additional measures for more sensitive information and the selected additional measures that will need to be strictly applied to control access to information marked OFFICIAL-SENSITIVE.

More detailed guidance on the security controls for NOMS information assets can be found in The IT Security Policy which relates specifically to ICT data, systems and hardware and The Information Assurance Policy which covers the wider controls required for both paper documents and ICT

Security handling guidance for different levels of classifications

	OFFICIAL	SECRET	TOP SECRET
DESCRIPTION of the classification	All information that is created, processed, generated, stored or shared within (or on behalf of) BIS is, at a minimum, **OFFICIAL**. **OFFICIAL – SENSITIVE** information is of a particularly sensitive nature. The "SENSITIVE" caveat should be used in limited circumstances (depending on the subject area, context and in some cases, any statutory or regulatory requirements) where there is a clear and justifiable requirement to reinforce the 'need to know'. Staff need to make their own judgements about the value and sensitivity of the information that they manage, in line with BIS and HMG corporate risk appetite decisions.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats.	The most sensitive information requiring the highest levels of protection from the most serious threats.
We protect this information from:	Hacktivists, single-issue pressure groups, private investigators, competent individual hackers and the majority of criminal individuals and groups.	As OFFICIAL plus state actors including defending against targeted and bespoke attacks.	All threat sources including sophisticated and determined state actors, and targeted and bespoke attacks.
Why do we protect this information?	▪ To meet legal and regulatory requirements. ▪ Promote responsible sharing and discretion. ▪ Implement proportionate controls appropriate to an asset's sensitivity. ▪ Make accidental compromise or damage unlikely.	*As OFFICIAL plus* ▪ To make accidental compromise or damage highly unlikely.	*As SECRET plus* ▪ To prevent unauthorised access.

	OFFICIAL	SECRET	TOP SECRET
IMPACT The compromise or loss would be likely to:	▪ Have damaging consequences for an individual (or group of individuals), or NOMS if lost, stolen or published in the media. ▪ Cause significant or substantial distress to individuals or a group of people. ▪ Break undertakings to maintain the confidence of information provided by third parties. ▪ Breach statutory restrictions on the disclosure of information. ▪ Undermine the proper management of the public sector and its operations. ▪ Shut down or substantially disrupt national operations. ▪ Seriously impede the development or operation of government policies. ▪ Substantially undermine the financial viability of major organisations. ▪ Impede the investigation or facilitate the commission of serious crime.	▪ Directly threaten an individual's life, liberty or safety. ▪ Seriously prejudice public order. ▪ Cause serious damage to the safety, security or prosperity of the UK. ▪ Cause substantial material damage to the national finances or economic or commercial interests. ▪ Cause serious damage to the effectiveness of extremely valuable security or intelligence operations. ▪ Cause major impairment to the ability to investigate serious organised crime. ▪ Cause serious damage to the security of Critical National Infrastructure.	▪ Threaten directly the internal stability, security or economic wellbeing of the UK or friendly nations. ▪ Lead directly to widespread loss of life. ▪ Cause exceptionally grave damage to relations with friendly nations. ▪ Cause exceptionally grave damage to the effectiveness of or intelligence operations. ▪ Cause long-term damage to the UK economy. ▪ Raise international tension. ▪ Cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations.
Examples	**OFFICIAL information** ▪ **All routine, day-to-day public sector business,** including policy development, service delivery, legal advice, personal data, staff reports, contracts, statistics, case files, and	▪ Information from or relating to security services or in relation to terrorist legal proceedings.	▪ Information from or relating to Security Services or in relation to terrorist legal proceedings.

	OFFICIAL	SECRET	TOP SECRET
	administrative data. ▪ Commercial information, including contractual information and intellectual property. ▪ Personal information that is required to be protected under the Data Protection Act. ▪ Procurement tenders, contracts and correspondence. ▪ Offender Case details involving individuals (except for cases where there is a real risk of harm or serious criminal activity may result from disclosure). ▪ Company information provided in confidence. ▪ Policy or operational minutes and papers. ▪ Honours nominations and deliberations. ▪ Threat assessments (and countermeasures) relating to the above level threats. **OFFICIAL – SENSITIVE 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 staff corruption investigations or other high profile or sensitive staff investigations. ▪ Highly sensitive personal data, such as information about	▪ Information relating to national security. ▪ Some Ministerial papers. ▪ Exchanging cryptographic materials. ▪ Key legal information / investigations.	▪ Information relating to counter-terrorism plans and policies. ▪ Information on national security.

	OFFICIAL	SECRET	TOP SECRET
	high profile offenders, VISOR data, extremism, and information relating to intelligence sources where it is not considered necessary to manage this information in the SECRET category.		
MARKING (of all material, whether paper, electronic, digital media)	There is **no requirement to mark** routine OFFICIAL information. In limited circumstances where there is a clear and justifiable 'need to know' requirement, the "SENSITIVE" caveat should be used. **OFFICIAL – SENSITIVE INFORMATION MUST ALWAYS BE CLEARLY MARKED.** Mark "OFFICIAL – SENSITIVE" in capital letters at the top and bottom of each document page, and in the Subject line and body of all emails. This could be followed by any handling or access requirements. **NOTE:** The originator is responsible for determining the appropriate classification for any assets they create. Depending on context and circumstances sensitivities may change over time and it may become appropriate to reclassify an asset. Only the originator can reclassify the asset.	**MUST ALWAYS BE MARKED.** Print "SECRET" in capital letters at the top and bottom of each page and on the front of folders, binders or notebooks, and in the Subject line and body of all emails.	**MUST ALWAYS BE MARKED.** Print "TOP SECRET" in capital letters at the top and bottom of each page and on the front of folders, binders or notebooks, and in the Subject line and body of all emails.
Marking handling instructions	All handling instructions or requirements as stipulated by the Information Asset Owner should be marked at the top and bottom of each document page, and at the beginning of any email message text.		

	OFFICIAL	SECRET	TOP SECRET
HANDLING OF INFORMATION YOU CREATE (of all material, whether paper, electronic, digital media)	**Handling instructions** are there to identify why special handling is required; who is to be allowed access to the information; how that information or data is allowed (or not) to be circulated or forwarded on and how it is to be stored. You control how the information you create is to be handled: you can describe any particular sensitivities of the information and offer meaningful handling advice. Additional handling instructions should be included following advice from the Information Asset Owner to identify handling requirements. Handling instructions should be included: ▪ On the front page of any document, and at the top of each page. ▪ As the first paragraph of any letter or minute. ▪ As the first paragraph of any email. ▪ Highlighted in the operations instructions for any dataset. **Basic formula for handling instructions**: <Reason this is classified as it is> <What you are allowed to do with this information> <What you need to do to ensure it is kept secure> **Example handling instructions:** • "Please do not distribute this document further." • "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."	*As for OFFICIAL*	*As for OFFICIAL*

	OFFICIAL	SECRET	TOP SECRET
	• "This information has been produced by NOMS. Do not share outside of NOMS without the written approval of the sender." • "To be opened by Addressee Only" – can be used for sending personal information for staff		
HANDLING OF INFORMATION (of all material, whether paper, electronic, digital media)	**You must follow any handling guidance stipulated by the Information Asset Owner.** You have a duty of confidentiality and a personal responsibility to safeguard any NOMS or MoJ information that you are entrusted with, or are handing to others. **OFFICIAL:** ▪ Lock computers when away from your desk. ▪ Adhere to the NOMS clear desk policy. **OFFICIAL – SENSITIVE:** *as OFFICIAL plus* ▪ Ensure documents are seen by, or passed to individuals only on a 'need to know' basis. **NOTES ON LEGACY INFORMATION:** ▪ Information or data marked under the previous protective marking scheme and still in use **does not** need to be remarked — provided that users / recipients understand how it is to be handled in line with this new Classification Policy. ▪ Any legacy information or data marked under the previous	**You must follow any handling guidance stipulated by the Information Asset Owner.** If applicable, additional handling instructions as for OFFICIAL should be included following advice from the Information Asset Owner to identify handling requirements (in the Subject line for an email; at the top of the page if a document). **Do not use QUANTUM / NICS / OMNI systems to transmit or store SECRET material.** *As OFFICIAL – SENSITIVE plus* ▪ Limit documents and movement of documents to those individuals who 'need	**You must follow any handling guidance stipulated by the Information Asset Owner.** If applicable, additional handling instructions as for OFFICIAL should be included following advice from the Information Asset Owner to identify handling requirements (in the Subject line for an email; at the top of the page if a document). **Do not use QUANTUM / NICS / OMNI systems to transmit or store TOP SECRET material.** *As OFFICIAL – SENSITIVE plus* ▪ Limit documents and movement of documents to those individuals who 'need

	OFFICIAL	SECRET	TOP SECRET
	protective marking scheme **does not** require remarking in line with this new Classification Policy.	to know'. ▪ Record movements of documents in a Classified Document Register (CDR). ▪ Always include a receipt with the document when moving documents. ▪ Line managers are to conduct monthly audit checks of the CDR and record the results in the CDR.	to know'. ▪ Record movements of documents in a Classified Document Register (CDR). ▪ Always include a receipt with the document when moving documents. ▪ Line managers are to conduct monthly audit checks of the CDR and record the results in the CDR.
Emailing material (inside the GSI / PSN or out over the Internet)	**OFFICIAL:** • You should not normally send work email to non-GSI/PSN/CJSM addresses unless allowed for under local business policies and procedures, or with Information Asset Owner approval. • Where more sensitive information must be shared with external partners (e.g. members of the public), consider using secure mechanisms such as password protection, consult IPA Team for advice. ▪ No restrictions on emailing information within secure systems, however it should be limited on a 'need to know' basis. ▪ You may choose to encrypt it to provide additional protection. Contact the IPA team for advice on encryption. ▪ You may choose to include additional handling instructions, if appropriate. ▪ You must follow any handling guidance stipulated by the	Not allowed	Not allowed

	OFFICIAL	SECRET	TOP SECRET
	Information Asset Owner. **OFFICIAL – SENSITIVE:** • You must only send work email to non-GSI/CJSM addresses unless allowed for under local business policies and procedures, or with Information Asset Owner approval ▪ "Release-Authorised:" must be the first words of the Subject line to signify that you have given thought to the sensitivity of the e-mail's contents and its destination. ▪ Information should normally be sent encrypted over the Internet. You can send it unencrypted over the Internet, but you have to make a risk-balanced decision and accept the risk of it being intercepted and exposed. When emailing OFFICIAL – SENSITIVE information within the department, you should still include the "Release-Authorised:" phrase in the Subject line.		
Moving assets by hand or post	**You must follow any handling guidance stipulated by the Information Asset Owner.** **BY HAND:** *OFFICIAL* ▪ Protected at least by one cover/envelope. ▪ Authorisation secured from the Information Asset Owner if moving a significant volume of assets / records / files. *OFFICIAL – SENSITIVE: as OFFICIAL plus* ▪ Carried in a nondescript bag in order to not draw attention	**You must follow the handling guidance as stipulated by the Information Asset Owner.** **Special handling arrangements need to be considered and advice must be obtained from the Department Security Officer (DSO).**	**You must follow the handling guidance as stipulated by the Information Asset Owner.** **Special handling arrangements need to be considered and advice must be obtained from the Department Security Officer (DSO).**

	OFFICIAL	SECRET	TOP SECRET
	to the contents. ▪ Never leave papers unattended. **BY POST/COURIER:** *OFFICIAL* ▪ Use single, unused envelope. *OFFICIAL – SENSITIVE: as OFFICIAL plus* ▪ Include return address on back of the envelope. ▪ Never mark the classification on envelope. ▪ Consider double envelope for highly sensitive assets (write the classification on the inner envelope only). ▪ Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service.		
Bulk transfer of documents/data	**You must follow any handling guidance stipulated by the Information Asset Owner.** ▪ Requires the approval of the Information Asset Owner. ▪ Assess for yourself the risks of transferring the assets. ▪ Conduct an appropriate risk assessment. ▪ Speak to the IPA team for the best course of action to take.	**You must follow the handling guidance as stipulated by the Information Asset Owner.** **Special handling arrangements need to be considered and advice must be obtained from the DSO.**	**You must follow the handling guidance as stipulated by the Information Asset Owner.** **Special handling arrangements need to be considered and advice must be obtained from the DSO.**
Faxing	**You must follow any handling guidance stipulated by the Information Asset Owner.** Faxes should not be assumed to be secure. Consider using	**Standard fax machines:** Not allowed. **Brent fax machines:** Allowed	**Standard fax machines:** Not allowed. **Brent fax machines:** Allowed

	OFFICIAL	SECRET	TOP SECRET
	encrypted email if possible to communicate sensitive information. **OFFICIAL:** ▪ No restrictions on faxing documents. **OFFICIAL – SENSITIVE:** ▪ Sensitive material to be faxed should be kept to an absolute minimum. ▪ Confirm the recipient's fax number. ▪ Recipients should be waiting to receive faxes containing personal data and/or data marked OFFICIAL – SENSITIVE.	only between Brent fax users (encrypted).	only between Brent fax users (encrypted).
Printing	**You must follow any handling guidance stipulated by the Information Asset Owner.** Permitted – but print only what you need. All printed materials must be disposed of appropriately when no longer required or being used.	Not allowed	Not allowed
Photocopying	**You must follow any handling guidance stipulated by the Information Asset Owner.** Permitted – but make only as many copies as you need, and control their circulation.	**Do not copy** SECRET documents without the appropriate authorisation from the originator.	Not allowed

	OFFICIAL	SECRET	TOP SECRET
STORAGE			
Physical storage (of documents, digital media, when not in use)	Protect physically within a secure building by a single lock (e.g. a locked drawer, container or locked filing cabinet). ▪ The clear desk policy should be observed. ▪ Papers should not be left on desks or on top of cabinets overnight. ▪ Laptops must be kept secure at all times and locked away overnight when left in the office.	**Special storage arrangements must be in place and advice must be obtained from the DSO.**	**Special storage arrangements must be in place and advice must be obtained from the DSO.**
Electronic storage on QUANTUM / NICS or OMNI	Permitted Any electronic document received marked OFFICIAL – SENSITIVE should be saved with OFFICIAL – SENSITIVE in the metadata, and appropriate controls used to limit access.	Not allowed	Not allowed
Electronic storage on digital media (USB memory sticks, CDs, DVDs)	Permitted ▪ The media must be encrypted. ▪ Only NOMS supplied and approved portable media is to be used.	Not allowed	Not allowed
Re-using digital media (USB memory sticks, CDs, DVDs)	For both OFFICIAL and OFFICIAL – SENSITIVE, delete contents and re-use digital media only within NOMS buildings and on NOMS computer systems.	▪ Users may delete and re-use the item themselves on the same stand-alone SECRET system. ▪ Digital media not to be reused on any other system	▪ Users may delete and re-use the item themselves on the same stand-alone TOP SECRET system. ▪ Digital media may not to be reused on any other

	OFFICIAL	SECRET	TOP SECRET
		unless securely wiped using an approved product. ▪ Digital media must be marked and treated as SECRET.	system, nor by other individuals. ▪ Digital media must be marked and treated as TOP SECRET.
Disposing of paper documents	Dispose of documents with care making reconstitution unlikely. **OFFICIAL:** tear the document into small pieces and place in a recycling bin. **OFFICIAL – SENSITIVE:** shred the document using an approved cross-cut shredder or place in a burn bag.	▪ Verify the document is complete with all pages present. ▪ Shred using a high-specification and approved cross-cut shredder. All shredding must be witnessed by another member of staff. ▪ Keep the waste secure; do not mark the bag containing the shredded material. ▪ Record the destruction of the document in the Classified Document Register, including two signatures (the person doing the destruction and a witness). ▪ Alternatively, use approved service providers.	▪ Verify the document is complete with all pages present. ▪ Shred using a high-specification and approved cross-cut shredder in the STRAP/TK Unit or using approved service providers. All shredding must be witnessed by another member of staff. ▪ Implement control measures to witness and record destruction. ▪ Record the destruction of the document in the Classified Document Register. ▪ Keep the waste secure; do not mark the bag containing the shredded material.
Disposing of digital media	**CDs and DVDs:** ▪ **Used for OFFICIAL information only:** Place disk into an	You must contact the IPA Team for advice at informationassurance@noms.	You must contact the IPA team for advice at informationassurance@noms.

	OFFICIAL	SECRET	TOP SECRET
(USB memory sticks, CDs, DVDs, etc)	envelope and break (with care) the disk into four pieces. Ensure that no piece is no larger than half of the total disc area. Dispose of pieces in ordinary office waste. Do not recycle. ▪ Used for OFFICIAL **– SENSITIVE** information: the disk should be shredded or ground and scrubbed, using an approved shredder or grinder. **USB memory sticks:** ▪ **Encrypted sticks:** Do not recycle, contact the IPA team for advice on appropriate methods of destruction. Shred any associated passwords. ▪ **Unencrypted memory sticks:** You must contact the IPA team.	gsi.gov.uk or on 0300 047 6590.	gsi.gov.uk or on 0300 047 6590. .
Disposing of hard disk drives	**Hard disk drive is to be / can be re-used** ▪ **OFFICIAL:** The hard disk drive should be overwritten using an approved commercial overwriting product. It can then be reused in an equivalent OFFICIAL environment. ▪ **OFFICIAL – SENSITIVE:** The hard disk drive should be Blanco'd, and then overwritten using an approved commercial overwriting product. It can then be reused in an equivalent classified environment. Depending upon the sensitivity of the information stored on the hard disk drive, it may be more appropriate to shred the disk when it is no longer needed. Please contact the IPA team for advice.	You must contact the IPA Team for advice at informationassurance@noms.gsi.gov.uk or on 0300 047 6590. .	You must contact the IPA Team for advice at informationassurance@noms.gsi.gov.uk or on 0300 047 6590.

	OFFICIAL	SECRET	TOP SECRET
	Hard disk drive no longer required and is not reusable ▪ Regardless of the information stored on it, the drive should be shredded by an approved commercial contractor. Please contact the IPA team for advice on this.		
REMOTE WORKING	▪ **Permitted following with the line manager's approval and compliance with the above guidance.** ▪ **No personal IT assets (eg, your home computer and peripherals) are to be used to process or store NOMS information.** ▪ Limit the amount of information you take out of the office. Only take what is necessary. ▪ Laptops and removable media used to store OFFICIAL and OFFICIAL – SENSITIVE information must be encrypted. ▪ Information must not be emailed to or from home e-mail accounts. **OFFICIAL:** ▪ Only encrypted, NOMS-supplied and approved portable media is to be used. ▪ Ensure information cannot be inadvertently overlooked. ▪ Store papers / portable media out of sight. ▪ NEVER leave papers or portable media in your car overnight. **OFFICIAL – SENSITIVE:** *as OFFICIAL plus* ▪ Items must not be opened or worked on whilst travelling or in a public area. ▪ Never leave papers / portable media unattended. ▪ If working from home, store papers, laptops and portable	▪ Secure agreement from the Information Asset Owner, who will carry out a risk assessment. ▪ Limit the amount of information you take out of the office. Only take what is necessary. ▪ Only carry in a locked container. ▪ The remote location must have a NOMS security-approved container to store material.	▪ Only to be removed for remote working as an exception if determined essential and following acceptance of the inherent risks by the DSO and senior management. ▪ Initial guidance should be sought from the NOMS STRAPSO.

	OFFICIAL	SECRET	TOP SECRET
	media in a locked drawer / cabinet.		
Discussing work on telephones (landline or mobile), in video conferences, via Microsoft Lync or in public places	**You should not assume telephony systems, video conferencing are secure.** **OFFICIAL:** ▪ No restrictions but be careful of straying into areas that could be deemed as OFFICIAL – SENSITIVE. **OFFICIAL – SENSITIVE:** ▪ Details of sensitive material should be kept to an absolute minimum.	Not allowed unless both parties are using encrypted equipment (e.g. Brent).	Not allowed unless both parties are using encrypted equipment approved to Top Secret (e.g. Brent).
PERSONNEL SECURITY	**OFFICIAL:** ▪ Prior to recruitment, HR / line managers should carry out appropriate recruitment checks to Baseline Personnel Security Standard (BPSS). ▪ Once recruited line managers should ensure staff complete the 'Responsible For Information' e-learning via Civil Service Learning. ▪ Line Managers should ensure that staff read the NOMS IPA team Intranet pages and know where to go if assistance is required. **OFFICIAL – SENSITIVE:** *as OFFICIAL plus* ▪ Staff should only share information on a 'Need to Know' basis.	▪ Prior to recruitment, HR / line managers should carry out appropriate recruitment checks. If regular uncontrolled access to SECRET is required, National Security Vetting (NSV) must be in place (Security Check, or SC) before the post-holder commences work. ▪ Once recruited line managers should ensure staff complete the 'Responsible For Information' e-learning via Civil Service Learning.	▪ Prior to recruitment, HR / line managers should carry out appropriate recruitment checks. If regular uncontrolled access to TOP SECRET is required, National Security Vetting (NSV) must be in place (Developed Vetting, or DV) before the post-holder commences work. ▪ Once recruited line managers should ensure staff complete the 'Responsible For Information' e-learning via Civil Service Learning.

	OFFICIAL	SECRET	TOP SECRET

		▪ Line Managers should ensure that staff read the BIS security pages on the intranet and know where to go if assistance is required.
		▪ Line Managers should:
		  ▪ enforce the 'Need to Know' principle; and
		  ▪ ensure special handling instructions are used (when appropriate).
			▪ Line Managers should ensure that staff read the BIS security pages on the intranet and know where to go if assistance is required.
			▪ Line Managers should:
			  ▪ enforce the 'Need to Know' principle;
			  ▪ be alert to any changes in staff behaviour;
			  ▪ ensure special handling instructions are used (when appropriate);
			  ▪ report concerns to the DSO; and
			  ▪ ensure regular aftercare.

Access requirements (clearance levels)	Baseline Personnel Security Standard (BPSS)	Security Check (SC) for regular, uncontrolled access. Staff with BPSS may see the occasional SECRET document when there is a 'Need to Know'.	Developed Vetting (DV) for regular, uncontrolled access. Staff with SC clearance may see the occasional TOP SECRET document when there is a 'Need to Know'.
INCIDENT REPORTING	▪ Inform the IPA team of any data loss / compromise at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590. ▪ Follow incident reporting procedures set out in the Information Assurance Policy	▪ Inform the IPA team of any data loss / compromise at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590.	▪ Inform the IPA team of any data loss / compromise at incidentreporting@noms.gsi.gov.ukor on 0300 047 6590.

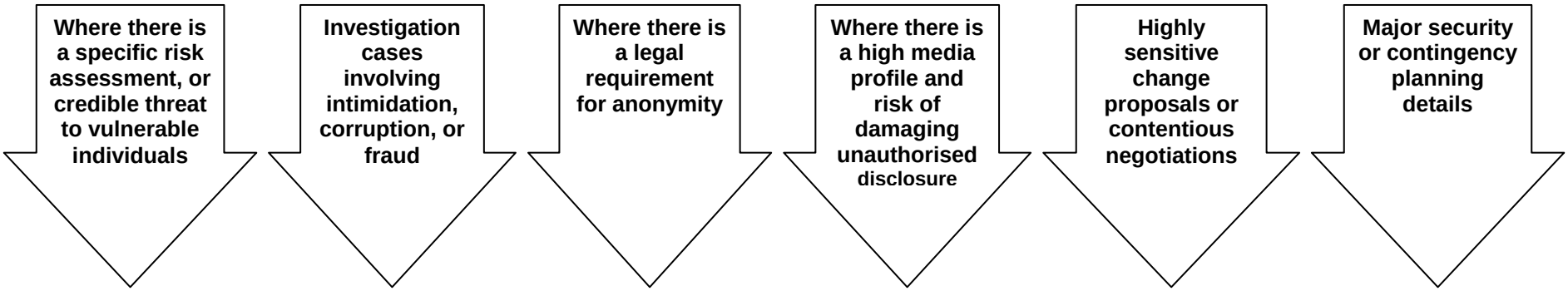
	OFFICIAL	SECRET	TOP SECRET
		▪ Follow incident reporting procedures set out in the Information Assurance Policy	▪ Follow incident reporting procedures set out in the Information Assurance Policy

Annex E

Official / Official Sensitive Guidance

OFFICIAL

- Staff HR records, including sick leave records and appraisals
- Offender records, including all reports, fingerprints, blood samples for pathology
- Financial data, including local budget information and staff payroll
- Purchasing, procurement, tendering, and contracts
- Health & Safety data, including workplace assessments, reports, and personal risk assessments
- Organisational information, including staff lists, business planning



OFFICIAL-SENSITIVE

- Information relating to ViSOR, staff corruption, high profile or sensitive investigations
- Contentious negotiations
- Major security or contingency planning issues
- Policy development and advice to Ministers on contentious and very sensitive issues e.g. Prison closures

Annex F

Contact details and where to find further information

Information Policy Assurance Team

To report a data loss / compromise:
incidentreporting@noms.gsi.gov.uk
0300 047 6590.

For advice and guidance on applying this policy:
informationassurance@noms.gsi.gov.uk
0300 047 6590

For guidance on the requirements and controls for Information Assurance:
The Information Assurance Policy

For guidance on the requirement and controls surrounding the use of ICT:
The IT Security Policy

Further guidance can be found on the government security classification scheme and other information matters can be found on the IPA team web pages at:

The Information Policy and Assurance Intranet Page at Change and ICT Communities