SCOTTISH FIRE AND RESCUE SERVICE
Working together for a safer Scotland

INFORMATION GOVERNANCE

GOVERNMENT SECURITY CLASSIFICATIONS POLICY

Original Author/Role	Lynne McAlonan, Information Security Officer
Date of Risk Assessment (if applicable)	N/A
Date of Equality Impact Assessment	In Progress
Date of Impact Assessment (commenced)	N/A
Date of Impact Assessment (concluded)	N/A
Quality Control (name)	Carol Wade, Information Governance Manager
Authorised (name and date)	Mark McAteer, Director of SPPC – August 2020
Date for Next Review	July 2026

VERSION HISTORY

Version	Change	Who	When
1.0	First version issued for familiarisation period	Lynne McAlonan, Information Security Officer	17/08/2020
-	Gone live	-	04/09/2020
2.0	Reviewed, no change to content – Date for Next Review and formatting updated	Lynne McAlonan, Information Security Officer	19/07/2023

CONTENTS

1. POLICY STATEMENT

2. PURPOSE OF THE POLICY

3. SCOPE

4. RESPONSIBILITIES

5. DEFINITIONS

6. SECURITY CLASSIFICATIONS AND PROTECTIVE MARKINGS

7. MARKING USING THE GOVERNMENT SECURITY CLASSIFICATION

8. WORKING WITH SECURITY CLASSIFICATIONS

9. SECURITY CONTROLS FRAMEWORK

10. COMPLIANCE WITH THE POLICY

11. LEGAL FRAMEWORK

12. RIGHTS TO ACCESS INFORMATION

13. ASSOCIATED DOCUMENTS / REFERENCES

APPENDIX A – PART 1 – THREAT MODEL AND SECURITY OUTCOMES

APPENDIX B – PART 2 – WORKING WITH ASSETS

1. POLICY STATEMENT

The Scottish Fire and Rescue Service (SFRS) is committed to ensuring that the appropriate level of protection is applied to all data and information and that consistent application of classification is applied to all data, information and documents to ensure compliance with relevant legislation and standards.

2. PURPOSE OF THE POLICY

The Cabinet Office has produced a Security Policy Framework for all Government Agencies and those who work in partnership with them, including Fire and Rescue Services. The Government Security Classifications 2018 (GSC) allows documents and data held to be classified according to the sensitivity and privacy relevant to it, enabling more efficient storage, security, distribution and destruction.

This Policy applies to all information that SFRS collects, stores, processes, generates or shares to deliver services or in the conduct of service business, including information received or exchanged with external partners.

This Policy provides all SFRS employees with the security classification categories and guidance on their application. It also provides guidance on the storage and dissemination of documents, data and information relevant to the security classification.

3. SCOPE

This Classification Policy applies to all SFRS employees, including contractors, agency staff and students. All data and information, including e-mails, maps, reports, spreadsheets, word documents, charts and drawings, whether stored electronically (including on removable media) and accessed via IT systems and applications or on paper, must be classified where required.

The GSC is intended to make it easier to classify information in a more meaningful way, improve sharing with external partners and make sure sensitive information receives the protection it needs.

4. RESPONSIBILITIES

All staff have a duty to respect the confidentiality and integrity of Service information and data to which they have access and are personally responsible for safeguarding.

The Chief Officer has overall responsibility for the implementation and compliance of this Policy.

All Line Managers are responsible for ensuring their staff are familiar with and fully understand this Policy for monitoring its compliance.

Line Managers are responsible for providing adequate change management processes to ensure mobility of staff without compromising the security of information. Where a role involves ownership of specific information and its classification, then any new member incumbent to that role must fully understand their responsibilities in this respect and must have appropriate authorised access clearance.

Information Owners are responsible for defining and periodically reviewing the classification of data and documents for which they are responsible. They are further responsible for ensuring that the sensitive documents they produce, whether created from existing electronic data or completely new, are adequately protected and marked with the appropriate classification.

Individual employees have responsibility for complying with this Policy and all related procedures.

5. DEFINITIONS

Government Security Classifications

A UK Government recognised system of marking documents and media to indicate their sensitivity. The descriptors used have very specific meanings which are recognised within Government, Police and Military agencies. Rules for storing and processing information with these classifications are set out by the Cabinet Office and must be complied with.

Classification

The process of grading documents according to their sensitivity.

Data / Information Owners

An individual who is responsible for ensuring that a particular information asset or group of assets is fit for purpose and meets organisational needs. This includes responsibility for applying appropriate classification and for determining an appropriate retention period.

Information Asset

A single piece of information or collection of information thought to be useful to the organisation.

Document Approvers

An individual who is responsible for approving a document.

ICT Application / Information system

Computer software that processes data to produce useable information that delivers against organisational needs.

Removable Media

USB sticks, CDs, DVDs, Mobile Technology, e g. Laptops, Smartphones, Tablets, etc.

6. SECURITY CLASSIFICATIONS AND PROTECTIVE MARKINGS

All information must be afforded a level of protection that is commensurate with its sensitivity. This is best determined by the data or information owners, as only they can have a full understanding of the consequences of its unauthorised or accidental disclosure or the implications of its loss or corruption. Having decided the level of protection required, using the guidance in this document, the data or information owner needs to communicate this to other individuals who, in the course of their duties, might handle, store or process the information. This is achieved by applying a consistent classification policy to all data, information and documents and an accompanying set of rules for their storage and processing.

There are 3 levels of protective marking within the GSC:

OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations 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 and highly capable threat actors. For example, where compromise could 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. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Note: 'Official-Sensitive' information is not a separate classification in its own right but applies to information that, although not Secret is too sensitive to remain merely as Official. This is akin to the old 'Confidential' level of information under the Government Protective Marking Scheme.

Information that is classified as OFFICIAL will not be physically marked but OFFICIAL-SENSITIVE and SECRET information will require a marking.

We do not currently store Top Secret information in SFRS and, therefore, there is no further reference to Top Secret in this document. Should you require any further information on the classification Top Secret, please do not hesitate to contact the Information Governance Manager or Information Security Officer at SFRSInfogov@firescotland.gov.uk

7. MARKING USING THE GOVERNMENT SECURITY CLASSIFICATION

OFFICIAL

ALL routine public sector business, operations and services should be treated as **OFFICIAL**. The majority of information assets created by SFRS are likely to be at this level. This includes a wide range of information of differing value and sensitivity, which needs to be defended against threats, such as activists, single issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups, and to comply with legal, regulatory and international obligations. This includes:

- The day-to-day business of SFRS, service delivery and public finances;
- Public safety, criminal justice and enforcement activities;
- Many aspects of security and resilience;
- Commercial interests, including information provided in confidence and intellectual property;
- Personal information that is required to be protected under GDPR and the Data Protection Act 2018.

Baseline Security Outcomes

- ALL SFRS information must be handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack;
- Staff must be trained to understand they are personally responsible for securely handling any information that is entrusted to them in line with business processes.

OFFICIAL-SENSITIVE

A limited subset of **OFFICIAL** information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the **OFFICIAL** classification tier but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked **OFFICIAL-SENSITIVE.**

Data Owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate.

To support specific business requirements and compartmentalise information, we may apply an optional DESCRIPTOR, alongside the **OFFICIAL-SENSITIVE** classification marking, to distinguish particular types of information and indicate the need for additional common sense precautions to limit access.

Examples of this are:

‘COMMERCIAL’: Commercial- or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to SFRS or to a commercial partner if improperly accessed.

‘PERSONAL’: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals or the personal/medical records of people.

SECRET

Very sensitive information that requires protection against threats such as sophisticated, well-resourced and determined threat factors, such as some highly capable serious organised crime groups.

Where the effect of accidental or deliberate compromise would be likely to result in any of the following:

- Directly threaten an individual’s life, liberty or safety;
- Cause serious damage to the operational effectiveness or security of the UK or allied forces such that, in the delivery of the military tasks:
    - Current or future capability would be rendered unstable;
    - Lives would be lost; or
    - Damage would be caused to installations rendering them unusable;
- Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations;
- Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction;
- Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests;

- Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets;
- Cause major impairment to the ability to investigate or prosecute serious organised crime.

All information in this security domain should be clearly and conspicuously marked **SECRET**. Information that requires more restrictive handling, due to the nature or source of its content, may merit a special handling instruction.

Baseline Security Outcomes

- Make accidental compromise or damage highly unlikely during storage, handling, use, processing, transmission, transport or disposal;
- Offer an appropriate level of resistance to deliberate compromise by forced and surreptitious attack;
- Where possible, detect actual or attempted compromise and help identify those responsible.

Should you require any further information on this, please do not hesitate to contact the Information Governance Manager or Information Security Officer at SFRSInfogov@firescotland.gov.uk

8. WORKING WITH SECURITY CLASSIFICATIONS

Security classifications can be applied to any asset that has value to the business. This includes information in whatever form (but not the IT systems used to store or process classified information), items of equipment, hardware and other valuables. Classification markings should be clear and conspicuous, including any special handling instructions.

When working with information assets, the following points need to be considered:

- There is no requirement to explicitly mark routine OFFICIAL assets;
- Over-classification involves marking information with a higher classification than is appropriate for the content. There is a risk that indiscriminate marking dilutes the impact of the secure categories. It could prevent access to information or documents required for effective service delivery and may also incur expense for secure resources that are not necessary;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise;
- When protecting an asset, typically a document, it must be clearly marked. Mark each page at the header using bold capital letters, for example **OFFICIAL-SENSITIVE**. File covers should be similarly marked. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions;
- Sensitive material published on intranet sites must also be clearly marked;
- It is good practice to reference the classification in the subject line and/or text of email communications. Where practicable, systems should compel users to select a classification before sending, e.g. via a drop-down menu;
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure, including release under Freedom of Information or to the National Archives;
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing OFFICIAL and SECRET material must be covered by the higher marking (i.e. SECRET);
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an email 'string' before they add to it and forward it on;
- In certain circumstances, there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement;

- Where practicable, time-expiry limits should be considered, so that protective controls do not apply for longer than necessary; this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics;
- Any document circulated internally within SFRS which has not been formally approved and signed off for issue should be marked 'DRAFT' in conjunction with the protective marking. This will indicate that the document is incomplete or not yet implemented. The protective marking assigned should be reviewed each time the draft is changed, to ensure the correct classification is still being applied. 'DRAFT' must be removed after the document is finalised and approved.

9. SECURITY CONTROLS FRAMEWORK

HMG Government Security Classification Policy has an Annex which describes the physical, personnel and information security controls required to provide a proportionate and robust level of protection for assets at each of the three classification levels (OFFICIAL, SECRET, TOP SECRET). SFRS have adopted several elements of this framework and have therefore provided appendices to provide further guidance to staff, rather than including further text in this policy.

Appendix A – Part 1 – Threat Model and Security Outcomes: providing the context and objectives underpinning risk management decisions.

Appendix B – Part 2 – Working with Working with Assets: typical security controls that individuals should apply when working with information (and other assets at each classification.

Within each level, assets must be protected to broadly consistent standards, wherever they are collected, stored, processed or shared across SFRS and with wider public sector and external partners. This consistency is essential to provide the confidence that underpins effective information sharing and interoperability between organisations.

10. COMPLIANCE WITH THE POLICY

The classification processes defined in this document are mandatory. From the date of implementation of this Policy, all new documents being produced and all existing documents which are revised should now be classified before being issued. The person creating or amending the document (Information Owner) must decide on the level of classification and apply it to the document. Document approvers shall ensure that a classification has been placed on a document before signing it off.

There is no requirement to re-classify information retrospectively.

If you require any assistance with this Policy, please do not hesitate to contact the Information Governance Manager or Information Security Officer at SFRSInfogov@firescotland.gov.uk

11. LEGAL FRAMEWORK

The UK classification system operates within the framework of domestic law. This includes:

Official Secrets Act 1989 (OSA): Damage assessment is a critical element of the OSA, most of the offences in which require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers or of confidential information received from a foreign State or an international organisation. With respect to each type of information, OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons under section 1 of the OSA; Crown servants; government contractors; and any person.

GDPR and Data Protection Act 2018 (DPA): The handling of personal data must be in compliance with DPA. The DPA, however contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA, such as the right of access to personal data. Departments and agencies should also have regard to the DPA, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

Freedom of Information Act (Scotland) 2002: Classification markings can assist in assessing whether exemptions to the Freedom of Information (Scotland) Act may apply. However, it must be noted that each FOI request may be considered on its own merits and the classification in itself is not a justifiable reason for exemption.

Public Records (Scotland) Act 2011: Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

12. RIGHTS TO ACCESS INFORMATION

Whole documents classified under the GSC, as detailed below, will not automatically become exempt from disclosure to the public. The Freedom of Information (Scotland) Act 2002, Environmental Information (Scotland) Regulations 2004, General Data Protection Regulations and the Data Protection Act 2018 provide rights for people to request information held by public authorities. If information which has been requested is contained within a classified document, consideration should be given to whether an exemption under the above legislation applies to that particular information or whether other parts of the document could be removed to allow the requested information to be released.

Advice on release of information must always be sought from the Information Governance Manager or the Data Protection / Freedom of Information Officers at SFRSInfogov@firescotland.gov.uk.

13. ASSOCIATED DOCUMENTS / REFERENCES

Government Security Classifications Policy Quick Guide

Acceptable Use Policy

Egress Switch Secure Email User Guide

Secure Desk Policy

Data Protection Act 2018

Environmental Information (Scotland) Regulations 2004

Freedom of Information Act (Scotland) 2002

General Data Protection Regulation 2018

HM Government Security Classifications 2018

Official Secrets Act 1989

Public Records (Scotland) Act 2011

APPENDIX A – PART 1 – THREAT MODEL AND SECURITY OUTCOMES

1. Security classifications indicate the sensitivity of information AND the typical controls necessary to defend assets against a broad profile of applicable threats. Risk owners should appreciate that information classified at one level cannot be assured to be protected against the threat profile associated with a higher level of classification.

OFFICIAL

2. The OFFICIAL tier provides for the generality of government business, public service delivery and commercial activity. This includes a diverse range of information, of varying sensitivities, and with differing consequences resulting from compromise or loss.

   OFFICIAL information must be secured against a threat model that is broadly similar to that faced by a large UK private company. This anticipates defending data and services against compromise by attackers with bounded capabilities and resources, including (but not limited to): hactivists, single-issue political pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

3. This model does not imply that information within the OFFICAL tier will not be targeted by some sophisticated and determined threat actors who may deploy advanced capabilities. It may be, rather, a risk-based decision has been taken not to invest in controls to assure protection against those threats, i.e. proportionate not guaranteed protection.

4. Technical controls at this level may be based on assured, commercially available products and services, without need for any bespoke development. Whilst these controls cannot absolutely assure against the most sophisticated and determined threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.

SECRET

5. The SECRET threat model anticipates a higher level of threat capability than would be typical for the threat model described in the OFFICIAL tier. The model includes threat sources, such as elements of serious and organised crime, as well as some state actors.

   Attacks may be bespoke in nature and tailored to specifically attack the target infrastructure. Vulnerable elements of the supply chain may be targeted to facilitate a further compromise of information. The opportunities for accidental compromise of information will be minimised with technical protection, where possible.

6. Risk owners should appreciate that assured protection will not be provided against very sophisticated, persistent and blended attacks by the most capable and determined organisations (such as highly competent state actors). A level of risk acceptance is required, that these threat sources have the capability to successfully target information within this tier, if they are motivated to do so.

TOP SECRET

7. The TOP SECRET threat model reflects the highest level of capability deployed against the nation's most sensitive information and services. Very little risk can be tolerated in this tier, although risk owners should note that no activity is entirely free from any risk.

Security Outcomes

To defend against these typical threat profiles, protective security controls should achieve the following outcomes at each classification level:

	OFFICIAL	**SECRET**	**TOP SECRET**
Outcome	• Meet legal and regulatory requirements • Promote responsible sharing and discretion • Proportionate controls appropriate to an asset's sensitivity • Make accidental compromise or damage unlikely	• Make accidental compromise or damage highly unlikely • Detect and resist deliberate attempts at compromise • Make it highly likely those responsible will be identified	• Prevent unauthorised access • Detect actual or attempted compromise • Identify those responsible and respond appropriately
Personnel Security	• Access by authorised individuals for legitimate business reasons	• Assurance that access is only by known and trusted individuals	• High assurance that access is strictly limited to known and trusted individuals
Physical Security (handling, use, storage, transport and disposal)	• Proportionate good practice precautions against accidental or opportunistic compromise • Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely	• Detect and resist deliberate compromise by forced and surreptitious attack • Destroy/sanitise to make reconstitution and/or identification of constituent parts highly unlikely	• Robust measures to prevent compromise by a sustained and sophisticated or violent attack • Destroy/sanitise to prevent retrieval and reconstitution
Information Security (storage, use, processing or transmission)	• Protect against deliberate compromise by automated or opportunist attack • Aim to detect actual or attempted compromise and respond	• Detect and resist deliberate compromise by sophisticated, determined and well-resourced threat actors	• Robust measures to prevent compromise from sustained attack by sophisticated, determined and well-resourced threat actors

APPENDIX B – PART 2 – WORKING WITH ASSETS

1. This section describes typical personnel, physical and information security controls required when working with assets. The indicative controls table should be used as the basis for local security instructions and processes.

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

3. Organisations may need to apply controls above (or below) the baseline to manage specific risks to particular types of information. Such exceptions must be agreed with the respective data owners and delivery partners. The SFRS SIRO will moderate any instances that entail pan-government risk.

4. Security requirements must be set out in local security instructions and reinforced by training to ensure that individuals understand their responsibilities. Organisations should operate an appropriate security culture commensurate with their particular circumstances and risk appetite.

5. Assets need to be managed to meet the following basic principles. More stringent controls may be appropriate to manage more sensitive assets:

    a. Handle with care to avoid loss, damage or inappropriate access. Compliance with applicable legal, regulatory and international obligations is the minimum requirement;
    b. Share responsibly, for business purposes. Use appropriately assured channels as required (e.g. secure email) and provide meaningful guidance on specific sensitivities and handling requirements;
    c. Store assets securely when not in use. For example, implement clear desk policies and screens locking when ICT is left unattended (refer to Acceptable Use Policy);
    d. Where assets are taken outside the office environment, they should be protected in transit, not left unattended and stored securely.

Precautions should be taken to prevent overlooking or inadvertent access when working remotely or in public places (refer to Secure Desk Policy);

e. When discussing SFRS business in public or by telephone, appropriate discretion should be exercised. Details of sensitive material should be kept to a minimum;

f. Particular care should be taken when sharing information with external partners or the public; for example, emails, faxes and letters should only be sent to named recipients at known addresses;

g. Information that is not freely available in the public domain should be destroyed in a way that makes reconstitution unlikely.

6. The table below describes standard control measures when working with information assets at each classification level. It should be read in conjunction with the detailed GSC Policy and other relevant SFRS guidance.

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
Overview	The majority of information that is created or processed by the public sector. This includes routine business operations 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.		Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.	The most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.
Threat Profile	Similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups. Many Government agencies and public sector organisations will operate exclusively at this level.		This anticipates the need to defend against a higher level of capability than would be typical for the OFFICIAL level. This includes sophisticated, well-resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors. Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks.	This reflects the highest level of capability deployed against the nation's most sensitive information and services. It is assumed that advanced state actors will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.
Definition	ALL routine public sector business operations and services should be treated as	A limited subset within OFFICIAL with more damaging consequences	Very sensitive information where the effect of accidental or deliberate compromise	Exceptionally sensitive information assets that directly support (or threaten)

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
	OFFICIAL. This includes: • The day-to-day business of government, service delivery and public finances; • Routine international relations and diplomatic activities; • Routine public safety, criminal justice and enforcement activities; • Many aspects of defence, security and resilience; • Routine commercial interests and information; • Personal information that is required to be protected under the Data Protection Act or other legislation (e.g. health records).	(individual or organisational) if compromised. The risk must be clear and justifiable, including: • Most sensitive corporate or operational information (e.g. organisational change planning, contentious negotiations, major security or business continuity); • Commercial or market sensitive information, including that subject to statutory or regulatory obligations; • Information about investigations and civil or criminal proceedings that could compromise public protection, enforcement or prejudice justice; • More sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but not appropriate for SECRET protections;	would be likely to result in any of the following: • Directly threaten an individual's life, liberty or safety (from highly capable threat actors); • Cause serious damage to the operational effectiveness or security of UK or allied forces; • Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations; • Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction; • Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests; • Cause serious damage to the security and resilience of Critical National Infrastructure	the national security of the UK or allies. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following: • Lead directly to widespread loss of life; • Threaten directly the internal stability of the UK or friendly nations; • Raise international tension; • Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks; • Cause exceptionally grave damage to relations with friendly nations; • Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations; • Cause long-term damage to the UK economy; • Cause major, long-term

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
		• Very sensitive personal data that may have severely damaging consequences through loss, but not required to manage as SECRET.	(CNI) assets; • Cause major impairment to the ability to investigate or prosecute serious organised crime.	impairment to the ability to investigate or prosecute serious organised crime.
Personnel Security	• Appropriate recruitment checks (e.g. the BPSS or equivalent); • Reinforce personal responsibility and duty of care through training.	• BPSS as minimum for regular, uncontrolled access; • 'Need to Know' principle applied.	• Always enforce 'Need to Know'' • Security Check for regular, uncontrolled access; • Special Handling Instructions.	• DV clearance for regular, uncontrolled access.
Handling	• General good practice approach such as clear desk/screen policy.	• Consider proportionate measures to control and monitor access.	• Register and file documents in line with locally determined procedures; • Maintain appropriate audit trails; • Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission; • Limit knowledge of planned movements to those with a need to know.	• Register movement of documents and undertake annual musters; • Conduct random spot checks of documents to ensure appropriate processing/handling/ record keeping and record results; • Strictly limit knowledge of planned movements to those with a need to know.
Storage	• General good practice administration should apply;	• Protect by single barrier and/or lock and key as minimum;	• Use of CPNI Approved Security Furniture; • Segregation of shared	• Use of CPNI Approved Security Furniture; • Robust measures to

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
	• Storage under single barrier and/or lock and key where possible.	• Consider use of appropriate physical security equipment/ furniture.	cabinets; • Proportionate measures to control and monitor access/movements	control and monitor movements; • Information must be accountable.
Movement	• Single cover; • Precautions against overlooking when working in transit; • Authorisation required for significant volume of records/files.	• Single cover; • Precautions against overlooking when working in transit; • Authorisation required for significant volume of records/files	• Risk assess the need for two people to escort the movement of document/media; • Documented local management approval required and completion of document/media removal/movement register; • Sealed tamper-evident container/secure transportation products; • Not accessed in public areas.	• Senior Manager approval subject to risk assessment
Transfer	• Post or courier; • Include return address, never mark classification on envelope.	• Post or courier; • Consider use of double envelope (protective marking on inner, return address on outer); • Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service.	• Local Management approval required, actions recorded in document movement register; • Robust double cover; • Approved registered mail service, commercial courier 'track and trace' service.	• Senior Manager approval subject to risk assessment; • Special handling arrangements may need to be considered.
Telephony, Video, Fax and	• Routine good administration applies	• Details should be kept to a minimum (use of guarded speech);	• Secure Telephony.	• Secure Telephony.

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
Airwave		• Recipients should be waiting to receive faxes; • Airwave is appropriately encrypted.		
Electronic Information at Rest	• Protected at rest by default (commercially available, appropriately assured, security products); • May be appropriate physical protection (such as data centre) or may involve Foundation Grade data at rest encryption.	• Data at rest on non-physically secure devices will be encrypted with Foundation Grade protection or other suitably assured products.	• Protected at rest by physical security appropriate for SECRET assets; • Data at rest on non-physically secure devices will be encrypted with (revitalised) Enhanced Grade protection.	• Protected at rest by physical security appropriate for TOP SECRET assets (SAPMA required); • Data at rest on non-physically secure devices will be encrypted with High Grade protection.
Electronic Information in Transit	• Information may be emailed/shared unprotected to external partners/citizens (subject to local business policies and procedures); • Personal information should be encrypted (essential in aggregate).	• Via accredited shared infrastructure, protected using Foundation Grade encryption or other approved encryption produce must be used – Switch Egress Secure Email; • Use secure mechanisms, such as client-side encryption or browser sessions using SSL/TLS.	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption; • Information will only be shared with defined users on appropriate and accredited recipient ICT systems.	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption; • Information will only be shared with defined users on appropriate and accredited recipient ICT systems.
Removable Media	• Any information moved to or transferred by removable media should be minimised to the extent	• Appropriate encryption should be used for temporary occasions; • Appropriate encryption	• Content must be appropriately encrypted unless (by exception) there exists appropriate	• Content must be appropriately encrypted unless (by exception) there exists appropriate

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET	TOP SECRET
	required to support the business requirement; • Consider appropriate encryption to protect the content, particularly where it is outside the organisation's physical control.	must be used for permanent/semi-permanent use.	full life physical protection.	full life physical protection.