Service Instruction 0816

Protective Marking – Government Security Classifications and Government Protective Marking Scheme

Document Control

Description and Purpose

This document is intended to advise on the principles the Government Security Classifications (GSC) and their application in Merseyside Fire and Rescue Authority. It also (by way of an appendix) provides guidance on the previous marking system, the Government Protective Marking Scheme (GPMS).

Active date	Review date	Author	Editor	Publisher
28.02.14	28.02.15	Deb Appleton	Deb Appleton	Sue Coker

Permanent		Temporary		If temporary, review date must be 3 months or less.
	X			

Amendment History

Version	Date	Reasons for Change	Amended by
1.0	11.03.14	Update to information on draft version & following consultation	Deb Appleton

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
	X	21.10.2013	Wendy Kenyon	Strategy & Performance/EIAs/Approved for Publish

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Policy	STRPOL14	Protective Security	Portal/Strategy & Performance/Polices & Service Instructions
Instruction	SI 0818	Personnel Security	Portal/Service Instructions
Policy	STRPOL09	Information Governance & Security Policy.	Portal/Strategy & Performance/Polices & Service Instructions
Instruction	SI 0675	Destruction of Confidential Waste	Portal/Service Instructions
Instruction	SI 0435	Data Protection Instructions	Portal/Service Instructions
Instruction	SI 0759	Destruction of Information Assets including Protectively Marked Information	Portal/Service Instructions

Contact

Department	Email	Telephone ext.
Strategy & Performance	debbieappleton@merseyfire.gov.uk	0151 296 4402

Target audience

All MFS	X	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

INTRODUCTION

Purpose

This Service Instruction (SI) is to advise on the principles the Government Security Classifications (GSC) and their application in Merseyside Fire and Rescue Authority. It also (by way of an Appendix) provides guidance on the previous marking system, the Government Protective Marking Scheme (GPMS).

The Authority recognises that information and information systems are valuable assets, which play a major role in supporting the organisation's strategic objectives. Information security is important for ensuring the safe and secure transaction of information for Authority business and the success of carrying out policy and administrative activities.

Information is a key asset and its correct handling is vital to the delivery of Fire and Rescue Authority services and to the integrity of those services. To strike the right balance between sharing and protecting information, the Authority needs to manage the business impacts and information risks associated with:

- Confidentiality – protecting information from unauthorised access and disclosure;
- Integrity – safeguarding the accuracy and completeness of information and processing methods; and
- Availability – ensuring that information and associated services are only available to authorised users when required

Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Introduction to Government Security Classifications and Government Protective Marking

Protective marking of information assets is an important part of Protective Security (see STRPOL14 Protective Security and also **STRPOL009_Information Governance and Security Policy**) as allows a co-ordinated way of implementing an appropriate level of protective controls against the likely threat to sensitive information. The threat may be posed by many agents including criminals, investigative journalists, pressure groups and protesters, terrorists, hackers, computer malware (e.g. viruses), natural disasters and disgruntled OR dishonest Staff members. The pace of technological developments also means that organisations need to be ever aware of new risks and threats.

The GSC Policy is in force from 2nd April 2014 and this describes how HM Government classifies information assets to ensure they are appropriately protected and will be adopted by MFRA. It will replace the Government Protective Marking Scheme. After 2nd April 2014 the GSC markings need to be applied to information assets including, documents, electronic records, email and audio visual material. However, it is important that both systems are understood as some *GPMS information assets will still exist within the organisation after implementation of the GSC Policy. An aide memoire for dealing with GPMS marked information can be found at **Appendix 1**

*For clarification any information assets marked PROTECT; RESTRICTED; CONFIDENTIAL are using the GPMS markings. SECRET and TOP SECRET are used by both systems.

Government Security Classifications

Using a protective marking system ensures that a protective marking is applied to a sensitive information asset to indicate its value in terms of the damage that is likely to result from that information being compromised. Protective marking is underpinned by the principal that information is only made available to those with a legitimate 'Need to Know'

The purpose of protective markings is to indicate the value of a particular asset in terms of the damage that is likely to result from its compromise. The GSC System ensures that sensitive information receives a uniform level of protection and treatment across Government, according to its degree of sensitivity.

The Government Security Classifications streamline the classification for information assets into three types:

OFFICIAL

SECRET

TOP SECRET

The majority of information assets held within the Authority are unlikely to require a classification above OFFICIAL or OFFICIAL - SENSITIVE, but a very small number of departments may deal with information marked SECRET. It is unlikely that any will deal with TOP SECRET information. However, some individuals may be in receipt of information from other agencies that does contain these higher levels of marking. Information that has been obtained from sources, which are publicly available, will not require a protective marking.

This Protective Marking SI sets out appropriate measures through which the Authority will classify its information to facilitate the secure handling, storage and disposal of its information assets.

For a summary view of the requirements for marking and processing GSC marked information see **Appendix 2.**

Viewing a Protectively Marked information asset

To view any protectively marked information an individual must have: -

A Need to know - this means that you should only see information that is related to your work
The appropriate level of security clearance (for further information see **Service Instruction SI 0818 Personnel Security**

Marking an Information Asset

Protective Marking should be considered by all staff when they create an information asset (for example, a document) when they have received guidance on how to do so. Only the originating organisation can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied. It is very important that, as an author, care be taken in selecting the appropriate protective marking. Information that is classified as OFFICIAL will not be physically marked, but OFFICIAL – SENSITIVE, SECRET and TOP SECRET information will require a marking.

Marking OFFICIAL - SENSITIVE, SECRET AND TOP SECRET: The latter two markings will be applied very rarely but OFFICIAL-SENSITIVE will be used more often. Any employees working with such documents can suggest a protective marking having applied the criteria, but the relevant Information Asset Owner and SMG member or Head of Department must approve that marking.

When protectively marking an asset, typically a document, it must be clearly and conspicuously marked. Mark each page at both the header and footer using bolded capital letters – for example **OFFICIAL - SENSITIVE**. File covers should be similarly marked. When marking e-mails put the marking in the subject or title box as well as in the message text, typically at the start or top of the e-mail.

Over classification should be avoided (eg classifying and marking a document as SECRET when it should be OFFICIAL and as a result, unmarked), as this risks introducing inefficiencies into the system, such as unnecessarily limiting access, increasing the costs of security controls needed to protect it and impairing business efficiency.

Equally, under classification should be avoided, which may put the asset at risk of accidental or deliberate compromise through inadequate protection.

Consider adding a time limit to the marking where the information asset will only require that marking for a short time, for example, information that is embargoed, but will be freely available once published.

Authors or owners of information assets should consider which of the following markings apply in every case and mark the asset accordingly.

Marking using the Government Security Classification

ALL routine public sector business, operations and services should be treated as **OFFICIAL**
The majority of information assets created by MFRA 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 MFRA,
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

OFFICIAL – SENSITIVE
This is subset of OFFICIAL is used by MFRA to mark assets that fall under the general classification of OFFICIAL but which require additional care in their handling and disclosure. These include:

- Very sensitive personal data. More routine personal data will be classified as OFFICIAL but in some cases may also carry a MFRA specific marking to indicate that it is required to be treated with confidentiality
- Commercial or marked sensitive information

In cases where OFFICIAL-SENSITIVE is considered the appropriate marking a descriptor can also be added to provide more information. For example “OFFICIAL-SENSITIVE Personal data” or “OFFICIAL-SENSITIVE commercial in confidence”.

SECRET

Very sensitive information that requires protection against threats such as sophisticated, well resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors.
and where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
b. Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:

    i. Current or future capability would be rendered unusable;
    ii. Lives would be lost; or,
    iii. Damage would be caused to installations rendering them unusable.

c. Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
d. Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.
e. Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.
f. Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
g. Cause major impairment to the ability to investigate or prosecute serious organised crime.

TOP SECRET
This reflects the highest level of capability deployed against the nation's most sensitive information and services. This covers exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies **AND** require extremely high assurance of protection. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Lead directly to widespread loss of life.
b. Threaten directly the internal stability of the UK or friendly nations.
c. Raise international tension.
d. 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.
e. Cause exceptionally grave damage to relations with friendly nations.
f. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

Storage of protectively marked information

Protectively marked information must not be left unattended during working hours when staff are away from their desks and are unable to lock the office/room. Protectively marked documents must not be taken out of the office unless appropriate security measures are in place. No protectively marked documents should be stored out of the office unless appropriate security containers and security alarms are fitted to the areas. The type of furniture needed to store protectively marked information in depends on the protective marking.

The following are minimum requirements:

Storage - Government Security Classifications

OFFICIAL

- Clear desk / screen policy
- Consider proportionate measures to control and monitor access to more sensitive assets
- Storage under single barrier and / or lock and key
- Consider use of appropriate physical security equipment / furniture (see the CPNI "Catalogue of Security Equipment", CSE)

SECRET

- 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
- Use of CPNI Approved Security Furniture
- Segregation of shared cabinets
- Proportionate measures to control and monitor access / movements

TOP SECRET

- 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
- Robust measures to control and monitor movements
- Information must be accountable

Electronic storage:

The security classification of electronic documents follows the same principles as that for hardcopy material and electronic documents must be protected in the same way.

Because of the differences between electronic and hardcopy documents, there are some extra steps needed to protect electronic data.

Protectively marked information on computer disk, CD, memory-stick or other electronic media must be marked with the security classification of the most highly classified data stored on the device. Protectively marked or sensitive information must only be stored on the MFRA network (subject to the restrictions outlined below) or on portable devices (such as memory sticks) provided by MFRA. This will ensure that sufficient levels of security are built in.

If there is a need to take protectively marked electronic documents away from the office, these must be protected in the same way as hardcopy material documents sharing the same classification. An encrypted device must be used for information marked at OFFICIAL- SENSITIVE

Electronic documents with a Government Protective Marking are also subject to Business impact Level restrictions:

The Business Impact levels

HMG IA Standard No.1 Business Impact Levels allow government organisations to consider the impact to business of unauthorised people; seeing information in a system (Confidentiality), changing information in a system (Integrity) and preventing access to information in a system (Availability).

For the previous Government Protective Marking Scheme there is a direct correlation between this and business impact level. The Government Protective Markings of PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET directly match to business impact levels 2, 3, 4, 5 and 6 respectively. This is a one-way relationship. It is not the case that an asset with a business impact level of 5 for confidentiality necessarily should be marked SECRET. This is especially true of impacts to aggregated data where large quantities of similar data are collected together and assigned an overarching impact level. In all cases, aggregation of significant amounts of data is likely to raise the impact level of its compromise.

The relevant business Impact Level for each of the Government Security Classifications has not been determined at time of writing. Until such a time as this is determined MFRA will assume that OFFICIAL could be IL2 or 3 and SECRET and TOP SECRET would be higher. As a result of current levels of network security, it would not be possible to store SECRET and TOP SECRET documents electronically on the network. Advice should be sought from the SIRO or Information Technology Security Officer.

MF&RS have controls in place: technical, people, policy, physical and assurance to handle information to BIL2 (Business Impact Level 2) – PROTECT.

There are risks associated with storing RESTRICTED Information on the existing MFRA network, sending it using MFRA Corporate E-Mail or accessing it on a USB stick from any MFRA PC or Laptop or indeed and PC or LAPTOP that has not been IL3 cleared. All systems at a level of BIL 3 or above must be formally accredited to HMG Information Assurance Standard No.2 (IS2). However the Authority does receive RESTRICTED information and it has been agreed that it can be held on the network as an interim solution. As soon as a BIL3 solution is available or the Business Impact Levels for the GSC have been published the situation will be reviewed. The exception to this is RESTRICTED information relating to national and local resilience which can be held on the National Resilience Extranet (NRE), an online private 'network' designed to enable civil protection practitioners to work together for emergency planning and incidents.

Communicating and Sharing Protectively Marked Information

Government Security Classifications

Email

OFFICIAL

- Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption.
- Information may be emailed / shared unprotected to external partners / citizens, subject to local business policies and procedures
- Where more sensitive information must be shared with external partners (e.g. citizens), consider using secure mechanisms (e.g. browser sessions using SSL / TLS

SECRET

- 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

TOP SECRET

- 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

OFFICIAL

- The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference
- Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement. Any removable media (eg a memory stick) must be encrypted and purchased through the ICT help desk. Encryption helps to protect the content, particularly where it is outside the organisation's physical control

SECRET

- Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

TOP SECRET

- Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

Telephone

OFFICIAL

- Details of sensitive material should be kept to a minimum.
- Recipients should be waiting to receive faxes containing personal data and / or data marked with the OFFICIAL – SENSITIVE caveat.

SECRET

- Secure Telephony, VTC and secure fax

TOP SECRET

- Secure Telephony, VTC and secure fax

Post

OFFICIAL

- Include return address, never mark classification on envelope
- Consider double envelope for sensitive assets
- Consider using registered Royal Mail service or reputable commercial courier's "track and trace" service

SECRET

- Local Management approval required, actions recorded in document movement register
- Robust double cover
- Approved registered mail service commercial courier ("track and trace"), or Government courier

TOP SECRET

- Security cleared (DV) diplomatically accredited courier only

Destruction of Protectively Marked Documents

Protectively marked documents should be reviewed regularly (ideally annually) to check whether they are still required. The relevant Retention Schedule should be consulted. Contact recordsmanagement@merseyfire.gov.uk for more information or refer to **Service Instruction 0687**. If a document is no longer required it should be destroyed using the right method for its classification, making sure that no one will be able to put it back together to read it. Consult **Service Instruction 0759 Destruction of Information Assets Waste including Protectively Marked Information** for more information.

If the information asset did not originate in MFRA the document should be returned to the provider or originator when it is no longer required (see section 5 above).

The way the document is destroyed will depend on its classification: -

Government Security Classifications

OFFICIAL
Dispose of with care using approved commercial disposal products to make reconstitution unlikely (refer to Centre for the Protection of National Infrastructure (CPNI) guidance and HMG IS5 Government guidance). Strategy and Performance Function will ensure that current arrangements are compliant and only suitable disposal products (eg cross cut shredders) will be available for purchase.

SECRET

- Consult the Senior Information Risk Owner (SIRO) - Verify document is complete before destruction
- Use Government approved equipment and or service providers.

TOP SECRET

- Consult the SIRO - Control measures will be used to witness and record destruction

Information losses/breaches

Any officer who becomes aware of the loss, theft or otherwise inappropriate disclosure of information marked OFFICIAL – SENSITIVE (Government Security classifications) or PROTECT or RESTRICTED (Government Protective Marking Scheme) should follow the process outlined in **Appendix 3**

Where the information asset is marked as CONFIDENTIAL, SECRET, TOP SECRET a different procedure must be followed. This is also outlined in **Appendix 3**.

Appendix 3 also contains details of the relevant Protective Security roles and the holders of those roles.

All reported breaches or potential weaknesses are investigated and, where necessary, further or alternative measures will be introduced to secure data. Such reports will be received by the Senior Information Risk Owner, the appropriate department head as necessary and in some cases, Government departments or the Police.

Disciplinary action could be taken depending on the circumstances of the loss or breach.

APPENDIX 1 - Aide Memoire for handling information marked using the Government Protective Marking Scheme

Storage of protectively marked information

Protectively marked information must not be left unattended during working hours when staff are away from their desks and are unable to lock the office / room. Protectively marked documents must not be taken out of the office unless appropriate security measures are in place. No protectively marked documents should be stored out of the office unless appropriate security containers and security alarms are fitted to the areas.

The type of furniture you need to store protectively marked information in depends on the protective marking. The following are minimum requirements:

PROTECT and RESTRICTED can be stored in any lockable furniture, within a secure building.

CONFIDENTIAL and SECRET must be stored in furniture locked with specific security keys or combinations as approved by Security Equipment Approved Panel (SEAP).

TOP SECRET documents must be stored in furniture locked with specific security devices, within a lockable room, with only a limited number of people permitted access to the room keys.

TOP SECRET and SECRET documents must be filed in numbered files or containers. It is useful to add a note of the file's contents so that individual files can be readily accessed when needed.

The security classification of electronic documents follows the same principles as that for hardcopy material and electronic documents must be protected in the same way. Most IT systems are not accredited to carry material protectively marked above PROTECT or RESTRICTED, and responders are encouraged to confirm with their information security officer the classification of material that may be stored on their system. Because of the differences between electronic and hardcopy documents, there are some extra steps needed to protect electronic data:

- Protectively marked information on computer disk, CD, memory-stick or other electronic media must be marked with the security classification of the most highly classified data stored on the device.
- Protectively marked or sensitive information must not be saved on a palm-held computer (PDA) ar a tablet unless provided by MFRA for the purpose.
- If there is a need to take protectively marked electronic documents away from the office, these must be protected in the same way as hardcopy material documents sharing the same classification.

Communicating and Sharing Protectively Marked Information

Email

There are specific rules for sending protectively marked information by email: -

Generally, NOT PROTECTIVELY MARKED and most PROTECT material may be transmitted across any internet email system. Where sensitive personal data (especially in aggregate) or material marked “PROTECT – PERSONAL DATA” is being sent by email, this data should be commercially encrypted (up to FIPS 140 standard). Email accounts that contain ‘gsi’ or ‘pnn’ in the address meet this standard.

Up to RESTRICTED may be sent between two systems accredited to communicate at this level (i.e.username@organisation.gsi.gov.uk to username@organisation.pnn.police.uk). If only one party has the necessary accredited system, then up to PROTECT only may be sent (subject to the caveat above regarding sensitive personal data).

Telephone

When you are dealing with information protectively marked RESTRICTED or above, you should not:

- Talk about it over a non-secure telephone line or non-secure mobile phone (unless it is RESTRICTED and your organisation has accepted the risk of so doing);
- Send it over a non-secure fax line (as above in regard RESTRICTED); or send it to a pager.

NOT PROTECTIVELY MARKED and PROTECT may be discussed / sent over non secure telephone / fax lines.

Post

A return address should always be included when sending protectively marked information by post. This is because all undelivered mail without a return address is opened at a Royal Mail sorting office where staff are not security cleared. The specific procedures for sending PROTECT, RESTRICTED and CONFIDENTIAL documents by post are:

- **PROTECT / RESTRICTED:** Address the envelope to an individual by name or job title and mark it 'Addressee only'. Do not include the classification on the envelope.
- **CONFIDENTIAL:** Follow the guidelines for RESTRICTED documents. When sending away from the building, the envelope must be marked CONFIDENTIAL and placed in a second envelope. Do not include the classification on the outer envelope.
- **SECRET / TOP SECRET:** Follow the guidelines for CONFIDENTIAL documents. Trusted hand delivery and special courier should be used for mail purposes.

Destruction of Protectively Marked Documents

You should review protectively marked documents regularly (ideally annually) to check whether you still need to keep them. If you no longer need a document, you should destroy it using to the right method for its classification, making sure that no one will be able to put it back together to read it. You should also record it in a registry (CONFIDENTIAL and higher). Alternatively, arrange for the document to be returned to the provider or originator.

The way you destroy the document will depend on its classification: -

- **PROTECT and RESTRICTED:** Use a cross cut shredder or put your documents in a confidential waste sack that is collected by an approved waste collector. This will make it unlikely that anyone will be able to read the information.
- **CONFIDENTIAL:** Tear up documents and place them in a confidential waste sack that is collected by an approved waste collector. Alternatively, shred as SECRET.
- **SECRET:** The documents should be shredded in a cross cutter; put the paper in at right angles to the print. The size of the shredded strips should be no more than 0.8mm and 12mm and not show more than two characters side by side. This will make it highly unlikely that anyone can put the document back together. When destroying SECRET documents, a record must be retained

of the date the document was destroyed and who authorised its destruction. This record must be kept for five years.

- **TOP SECRET:** These documents must be destroyed in the same way as SECRET documents, except that two people must witness the shredding and sign the registry.

Also consult the MFRS **Service Instruction SI 0675 Destruction of Confidential Waste**

http://intranetportal/sites/cc/Service%20Instructions1/Service%20Instructions/SI%200675%20Destruction%20of%20Confidential%20Waste.doc

HMG IA Standard No. 5 - Secure Sanitisation also provides comprehensive guidance

APPENDIX 2 - Government Security Classifications – Matrix V1.0

	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 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	A limited subset within OFFICIAL with more damaging consequences (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	Very sensitive information 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 (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	Exceptionally sensitive information assets that directly support (or threaten) 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,

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
	Data Protection Act (1998) or other legislation (e.g. health records).	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 • Very sensitive personal data, that may have severely damaging consequences through loss, but not required to manage as SECRET	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.	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 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' • SC for regular, uncontrolled access • Special Handling Instructions	• DV 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 • Storage under single barrier and / or lock and key where possible	• Protect by single barrier and / or lock and key as minimum • Consider use of appropriate physical security equipment / furniture	• Use of CPNI Approved Security Furniture (SAPMA required) • Segregation of shared cabinets • Proportionate measures to control and monitor access / movements	• Use of CPNI Approved Security Furniture (SAPMA required) • Robust measures to 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(s)/media • Documented local management approval required and completion	• Senior Manager approval subject to risk assessment

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
			of document / media removal / movement register • Sealed tamper-evident container / secure transportation products (refer to CSE) • Not accessed in public areas	
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 couriers '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 Airwave	• Routine good administration applies	• Details should be kept to a minimum (use of guarded speech) • Recipients should be waiting to receive faxes • Airwave is appropriately encrypted	• Secure Telephony, VTC and secure fax (BRENT)	• Secure Telephony, VTC and secure fax (BRENT)
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 (SAPMA required) • 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 (such as PSN), protected using Foundation Grade encryption, or other approved encryption product must be used (CJSM/NRE etc.) • 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 required to support the business	• Appropriate encryption should be used for temporary occasions • Appropriate encryption must be	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
	requirement • Consider appropriate encryption to protect the content, particularly where it is outside the organisations physical control	used for permanent / semi-permanent use		

APPENDIX 3 – Process for handling information losses/breaches (including inappropriate disclosure of information)

Also see Service instruction SI 0435 Data Protection Instructions

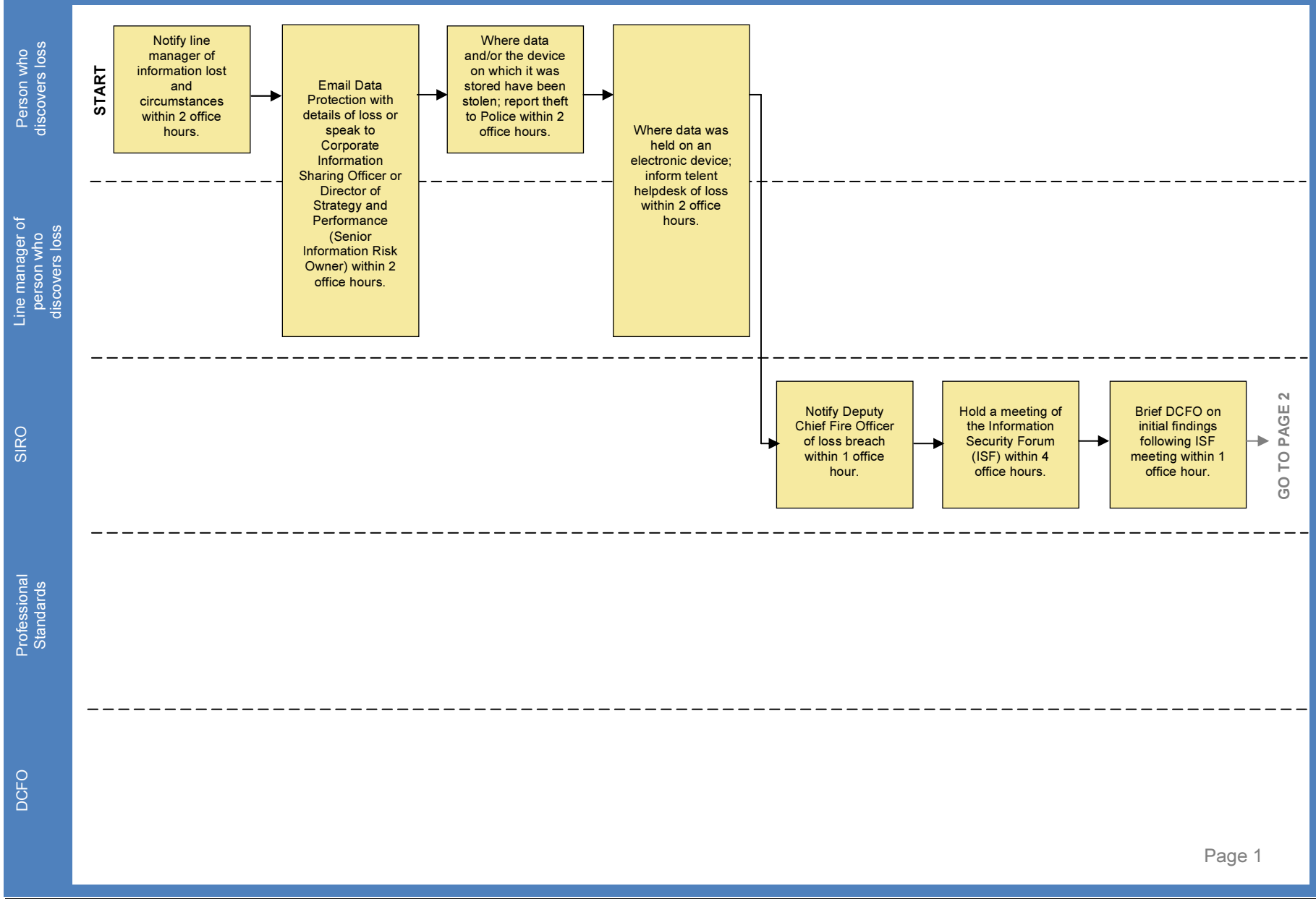
*Office hours. Out of hours response will be considered on a case by case basis

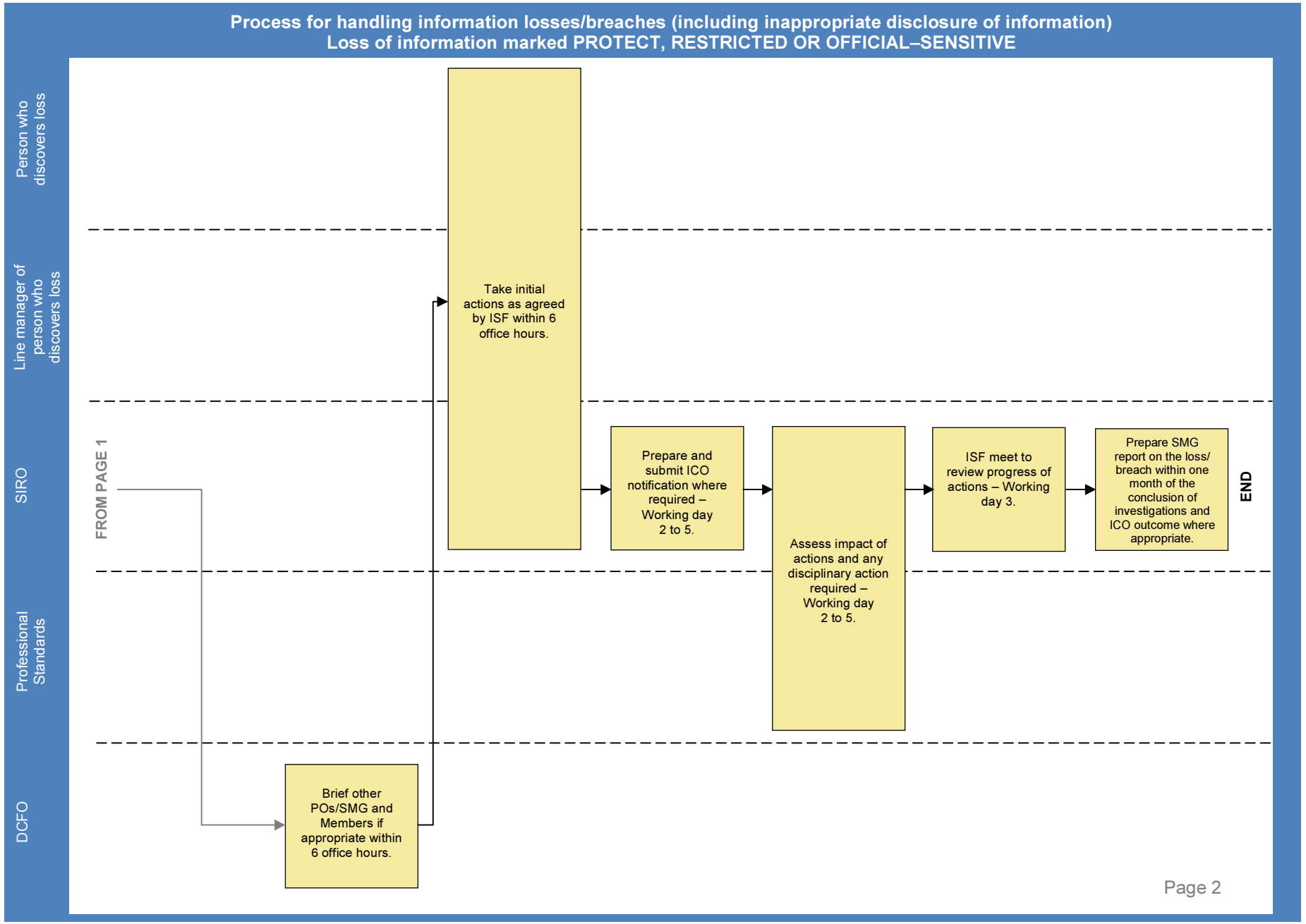
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL - SENSITIVE			
	Action	**Responsible person**	**Timescale**
1	Notify line manager of the information lost and the circumstances	Person who discovers the loss	At the first opportunity following discovery of the loss – within *2 hours
2	Either Email dataprotection@merseyfire.gov.uk with details of the loss or ring 0151 296 4479/4474 and speak to the Corporate Information Sharing Officer or 07818 034982 for the Director of Strategy and Performance (Senior Information Risk Owner)	Person who discovers the loss or their line manager	At the first opportunity following discovery of the loss – *2 hours
3	Where the data and/or the device on which it was stored have been stolen; report the theft to the Police.	Person who discovers the loss	At the first opportunity following discovery of the loss – within *2 hours
4	Where the data was held on an electronic device; contact the telent helpdesk to inform them of the loss	Person who discovers the loss or their line manager	At the first opportunity following discovery of the loss – within *2 hours
5	Senior Information Risk Owner (SIRO) notifies the Deputy Chief Fire Officer of the loss breach	SIRO	At the first opportunity following notification – within *1 hour
6	SIRO holds a meeting of the Information Security Forum (ISF) to consider the following: • What has been lost – are further investigations necessary (Service Security Officer to be involved)?	SIRO	Within *4 hours of notification

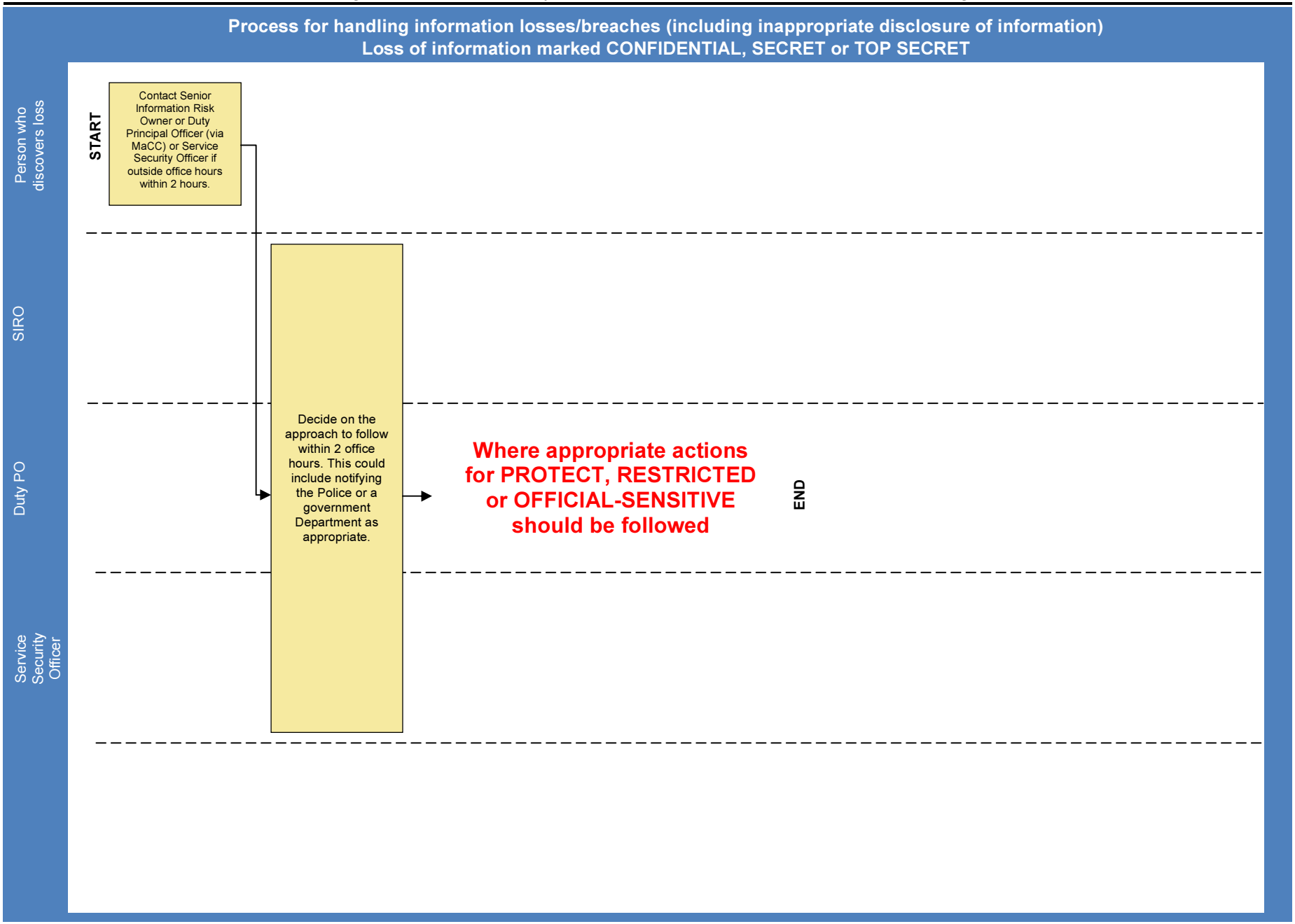
	• whether the information "belongs" to MFRA • Potential damage to the organisation concerned or individuals and how they will be informed • Is notification to the Information Commissioners Office (ICO) required? • Is there an insurance implication? • What immediate message needs to be sent to staff/public (Corporate Communications to be advised) • Consider level of police involvement		
7	SIRO briefs the DCFO on the initial findings	SIRO/DCFO	Following ISF meeting – within *1 hour
8	DCFO briefs other POs/SMG and Members if appropriate	DCFO/SIRO	Within *6 hours of notification
9	SIRO and notifying officer/line manager take initial actions as agreed by ISF	SIRO/notifying officer/ line manager	Start within *6 hours of notification
10	SIRO prepares and submits ICO notification where required	SIRO	Day *2 to 5
11	SIRO assesses impact of actions and any disciplinary action required – with Professional Standards.	SIRO/Professional Standards	Day *2 to 5
12	ISF meets to review progress of actions	SIRO	Day *3
13	SIRO prepares SMG report on the loss/ breach	SIRO	Within one month of the conclusion of investigations and ICO outcome where appropriate

Loss of Information marked CONFIDENTIAL, SECRET or TOP SECRET			
	Action	**Responsible person**	**Timescale**
1	Contact the Senior Information Risk Owner or Duty Principal Officer (via MaCC) or Service Security Officer if outside office hours.	Person who discovers the loss	At the first opportunity following discovery of the loss – within 2 hours
2	A decision will then be taken on the approach to follow. This could include notifying the Police or a government Department as appropriate.	SIRO/Duty PO/Service Security Officer	Within 2 hours of notification
3	Where appropriate, the above actions for PROTECT, RESTRICTED or OFFICIAL-SENSITIVE will be followed in addition to any specific actions determined in 3.	SIRO	In accordance with timescale for PROTECT, RESTRICTED and OFFICIAL-SENSITIVE
	Protective Security roles: **Protective Security Lead** Phil Garrigan - Deputy Chief Fire Officer **Service Security Officer** (SSO) - (TBC) **Information Technology Security Officer** (ITSO) - Mark Hulme – ICT Applications Manager **Senior Information Risk Owner** (SIRO) Deb Appleton – Director of Strategy and Performance **Information Asset Owners** (IAO) – there is at least one IA in each department. Contact the SIRO for further details		

Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL–SENSITIVE




Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL–SENSITIVE
Person who discovers loss
Line manager of person who discovers loss
SIRO
Professional Standards
DCFO
FROM PAGE 1
Take initial actions as agreed by ISF within 6 office hours.
Prepare and submit ICO notification where required – Working day 2 to 5.
Assess impact of actions and any disciplinary action required – Working day 2 to 5.
ISF meet to review progress of actions – Working day 3.
Prepare SMG report on the loss/ breach within one month of the conclusion of investigations and ICO outcome where appropriate.
END
Brief other POs/SMG and Members if appropriate within 6 office hours.
Page 2


Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked CONFIDENTIAL, SECRET or TOP SECRET
Person who discovers loss
SIRO
Duty PO
Service Security Officer
START
Contact Senior Information Risk Owner or Duty Principal Officer (via MaCC) or Service Security Officer if outside office hours within 2 hours.
Decide on the approach to follow within 2 office hours. This could include notifying the Police or a government Department as appropriate.
Where appropriate actions for PROTECT, RESTRICTED or OFFICIAL-SENSITIVE should be followed
END