

Handling Protectively Marked Material

A Guide for Police Personnel

PROTECT
RESTRICTED
CONFIDENTIAL
SECRET
TOP SECRET



Revised April 2007

Introduction

The Chief Constables' Council originally mandated adoption of the Government Protective Marking Scheme in 2001. This is now a formal compliance requirement of the ACPO/ACPOS Information Systems Community Security Policy.

This guidance leaflet supersedes and replaces the previous issue dated October 2001.

Personnel need to be aware that it is important that protective security practices:

- Implement the 'need to know' principle
- Are workable and user-friendly
- Deal with all the prevailing threats
- Are effectively co-ordinated by the Personnel who use them
- Are just, open and reasonable, where they may impinge on the lives of staff

When selecting the appropriate marking, personnel should also consider:

- How damaging the consequences would be if material was lost, stolen, disclosed or destroyed
- Correct marking is applied (over or under classification damages the credibility of the system)
- A compilation of many items marked at the same level may require the whole to be marked at a higher level
- The scheme should not be used to protect against sensitivities likely to arise due to inefficiency or administrative error

- It does not provide exemption from Freedom of Information legislation
- Regular reviews of the material may be necessary in order to downgrade or destroy any such material

As from February 2007 there are now five levels of Protective Marking* that can be applied to sensitive assets, depending on the degree of sensitivity involved:

1. **PROTECT**
2. **RESTRICTED**
3. **CONFIDENTIAL**
4. **SECRET**
5. **TOP SECRET**

The majority of information held within the Police Service contains personal or sensitive data and therefore requires a level of Protective Marking.

(Information already in the public domain will not require a protective mark.)

This guide predominantly deals with assets that are marked at either PROTECT, RESTRICTED or CONFIDENTIAL, as they comprise the vast majority of 'sensitive' information assets held within the Police Service.

It is intended to give very basic guidance on the application of protective markings to **police information** together with storage handling and movement requirements.

It is not exhaustive! For further clarification and in particular for advice regarding SECRET and TOP SECRET please contact your Information Security Officer.

**NB – When used as a Protective Marking – the words PROTECT / RESTRICTED / CONFIDENTIAL / SECRET and TOP SECRET, will be displayed in capitals to differentiate them from ordinary use within documents. The same rule applies when attaching a descriptor (see later) all DESCRIPTORS will be written in capital letters.*

Impact Criteria – Public Order, Public Safety and Law Enforcement

<h2>PROTECT</h2> <p>Impact Levels 1 & 2</p> <p>Would accidental or deliberate compromise of assets marked PROTECT be likely to cause:</p> <p>Impact Level 1</p> <ul style="list-style-type: none"> ◆ No impact on life and safety; ◆ Minor disruption to emergency service activities that requires reprioritisation at local (station) level to meet expected levels of service; ◆ No impact on crime fighting; ◆ No impact on judicial proceedings; <p>Impact Level 2</p> <ul style="list-style-type: none"> ◆ Inconvenience or cause discomfort to an individual; ◆ Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service; ◆ Minor failure in local Magistrates Courts <p style="text-align: center;">NOTE</p> <ul style="list-style-type: none"> ◆ PROTECT is not a national security protective marking and the policy relating to the use of RESTRICTED remains unchanged. ◆ Not to be used for operational issues. ◆ Must be accompanied by a Descriptor, (e.g. PROTECT – STAFF). 	<h2>RESTRICTED</h2> <p>Impact Level 3</p> <p>Would accidental or deliberate compromise of assets marked RESTRICTED be likely to cause:</p> <ul style="list-style-type: none"> ◆ A risk to an individual's personal safety or liberty ◆ Disruption to emergency service activities that requires reprioritization at the County or organizational level to meet expected levels of service ◆ Hinder the detection, impede the investigation of, or facilitate the commission of low level crime (i.e. crime not defined in legislation as "serious crime"), or hinder the detection of serious crime ◆ A low-level criminal prosecution to collapse; cause a conviction for a low-level criminal offence to be declared unsafe or referred for appeal ◆ A breach of proper undertakings to maintain the confidence of material provided by third parties; ◆ A breach of statutory restrictions on disclosure of material (does not include the Data Protection Act 1998, where <u>non</u>-sensitive information is involved); ◆ An undermining of confidence in public services; 	<h2>CONFIDENTIAL</h2> <p>Impact Level 4</p> <p>Would accidental or deliberate compromise of assets marked CONFIDENTIAL be likely to cause:</p> <ul style="list-style-type: none"> ◆ A risk to a group of individuals safety or liberty; ◆ Disruption to emergency service activities that requires reprioritization at national level (e.g. one police force requesting help from another) to meet expected levels of service; ◆ Impeding of the investigation of, or facilitate the commission of serious crime (as defined in legislation); ◆ A serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred to appeal; <h2>TOP SECRET</h2> <p>Impact Level 6</p> <p>Would accidental or deliberate compromise of assets marked TOP SECRET be likely to:</p> <ul style="list-style-type: none"> ◆ Lead directly to widespread loss of life; ◆ Threaten directly the internal stability of the UK or friendly countries leading to widespread instability; ◆ Cause major, long term impairment to the ability to investigate serious organised crime (as defined in legislation); ◆ Cause the collapse of the UK Judicial system; 	<h2>SECRET</h2> <p>Impact Level 5</p> <p>Would accidental or deliberate compromise of assets marked SECRET be likely to cause:</p> <ul style="list-style-type: none"> ◆ A threat to life directly leading to limited loss of life; ◆ Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency service) to meet expected levels of service; ◆ Major, long term impairment to the ability to investigate serious crime (as defined in legislation); ◆ A number of criminal convictions to be declared unsafe or referred to appeal (e.g. through persistent and undetected compromise of an evidence-handling system);
--	--	--	--

'Protective Marking' is the method by which the **originator** of an asset (that is all material assets, ie papers, drawings, images, disks and all forms of electronic data records), indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within and outside the originator's own department or force and its ultimate method of disposal.

When a protective marking is applied to an information asset it is indicating its value in terms of the damage that is likely to result from that information being compromised. The sections on this page detail the criteria **specific to public order, public safety and law enforcement** for each level of Protective Marking.

Impact Criteria – Defence, International Relations and Intelligence

PROTECT

Impact Levels 1 & 2

Would accidental or deliberate compromise of assets marked **PROTECT** be likely to cause:

Impact Level 1

- ◆ Delay or loss of minor supply service;

Impact Level 2

- ◆ Inconvenience or cause discomfort to an individual;
- ◆ The loss of a number of minor supply services;

RESTRICTED

Impact Level 3

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to cause:

- ◆ A risk to an individual's personal safety or liberty;
- ◆ Minor loss of confidence in Government;
- ◆ More difficulty to maintain the operational effectiveness of security of UK or allied forces (e.g. compromise of UK forces doctrine or training materials);
- ◆ Embarrassment to Diplomatic relations;
- ◆ Disadvantage to a major UK company;
- ◆ Damage to unique intelligence operations in support of intelligence requirements at JIC Priority Three or less;

CONFIDENTIAL

Impact Level 4

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to cause:

- ◆ A risk to a group of individuals safety or liberty;
- ◆ Major loss in confidence in Government;
- ◆ Damage to the operational effectiveness of security of UK or allied forces (e.g. compromise of a logistics system causing re-supply problems without causing risk to life);
- ◆ Disadvantage to a number of major UK Companies;
- ◆ A halt in unique intelligence operations in support of intelligence requirements at JIC Priority Three or less, or damage unique intelligence operations in support of intelligence requirements at JIC Priority Two;

SECRET

Impact Level 5

Would accidental or deliberate compromise of assets marked **SECRET** be likely to cause:

- ◆ A threat to life directly leading to limited loss of life;
- ◆ A direct threat to the internal political stability of the UK or friendly countries;
- ◆ Severe damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of company size or below in a theatre of military operations);
- ◆ A rise in international tension, or seriously damage relations with friendly governments;
- ◆ Disadvantage to the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a bilateral trade dispute);
- ◆ A halt in unique intelligence operations in support of intelligence requirements at JIC Priority Two, or damage unique intelligence operations in support of intelligence requirements at JIC Priority One;

TOP SECRET

Impact Level 6

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to:

- ◆ Lead directly to widespread loss of life;
- ◆ The collapse of internal political stability of the UK or friendly countries
- ◆ Cause exceptionally grave damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of battalion size or above in a theatre of military operations)
- ◆ Directly provoke international conflict, or cause exceptionally grave damage to relations with friendly governments
- ◆ Severely disadvantage the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a major EU or WTO negotiating round)
- ◆ Halt unique intelligence operations in support of intelligence requirements at JIC Priority One.

Impact Criteria – Critical National Infrastructure

PROTECT

Impact Levels 1 & 2

Would accidental or deliberate compromise of assets marked **PROTECT** be likely to cause:

Impact Level 1

- ◆ Local loss of telecoms for a few hours;
- ◆ Local power outages causing disruption for up to 12hours;
- ◆ Minimal impact on finance (less than £10,000);
- ◆ Minor disruption of a key local transport systems for up to 12 hours
- ◆ The breakdown of local water supplies and/or sewage service for a small number (<10) of people for more than a day;
- ◆ Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food of up to a week;

Impact Level 2

- ◆ Local loss of telecoms for up to 12 hours;
- ◆ Local power outage causing distribution for up to 24hours;
- ◆ Minor loss to a Financial Company (less than £1 million);
- ◆ Minor disruption of key local transport systems for up to 24 hours;
- ◆ The breakdown of local water supplies and/or sewage service for a small number (<50) of people for more than a week;
- ◆ Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or disruption of food for up to a month;

RESTRICTED

Impact Level 3

Would accidental or deliberate compromise of assets marked **RESTRICTED** be likely to cause:

- ◆ Local loss of telecoms for up to 24 hours;
- ◆ Loss of power in a region causing disruption for up to 24 hours;
- ◆ Major loss of a Leading Financial company of £millions;
- ◆ Disruption of a number of key local transport systems for up to 24 hours;
- ◆ Breakdown of local water supplies and/or sewage service for a number (up to 100) of people or prolonged drought (up to 1 months);
- ◆ Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and/or widespread disruption of food for up to a week;

CONFIDENTIAL

Impact Level 4

Would accidental or deliberate compromise of assets marked **CONFIDENTIAL** be likely to cause:

- ◆ Loss of telecoms of a region for up to 24 hours;
- ◆ Loss of power in a region causing disruption for up to a week;
- ◆ Major loss of a Leading Financial Company of £10s millions;
- ◆ Major disruption of key regional transport systems for up to a week;
- ◆ Breakdown of local water supplies and/or sewage service for over 100 people or prolonged drought (up to 1 month);
- ◆ Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month;

SECRET

Impact Level 5

Would accidental or deliberate compromise of assets marked **SECRET** be likely to cause:

- ◆ Loss of telecoms nationally for up to a week;
- ◆ Loss of power in a region causing distribution for more than 1 week;
- ◆ Severe losses to UK Business of up to £1 billion;
- ◆ Severe national disruption of key transport systems for up to a week;
- ◆ Breakdown of regional water supplies and/or sewage service (effecting >100 people) or prolonged drought (up to 3 months);
- ◆ National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month;

TOP SECRET

Impact Level 6

Would accidental or deliberate compromise of assets marked **TOP SECRET** be likely to cause:

- ◆ Loss of telecoms nationally for more than 1 week;
- ◆ Loss of power nationally affecting the whole of the UK for more than 1 week;
- ◆ Severe financial losses to UK Business of £10s billions;
- ◆ Severe national disruption of key transport systems for over a month;
- ◆ Total breakdown of national water supplies and/or sewage service (effecting >100 people) or prolonged drought (> 6 months);
- ◆ National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for over a month;

Handling, Storage and Movement

Application / Activity	PROTECT	RESTRICTED	CONFIDENTIAL
Marking documents	Top and bottom of every page	Top and bottom of every page	Top and bottom of every page
Storage of hard copy documents	Protected by one barrier, e.g. a locked container within a secure building.	Protected by one barrier, e.g. a locked container within a secure building.	Protected by two barriers e.g. a locked container in a locked room, within a secure building.
Disposal of paper waste	Use secure waste sacks. Keep secure when left unattended.	Use secure waste sacks. Keep secure when left unattended.	Use a SEAP approved cross cut shredder. Keep secure when left unattended.
Disposal of magnetic media	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk - dismantle and cut disk into quarters & dispose with normal waste. Optical Media - destroy completely - disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.
Reuse of Media (Hard Drives etc)	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.
Movement within Force using own internal distribution system	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.	In a new sealed envelope with protective marking shown. Transit envelopes must not be used.
Movement between forces/partner agencies	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.	By post or courier. Double enveloped both fully addressed. Protective marking shown on inner envelope only. Return address on outer envelope.
Force Internal 'Phone Network	May be used.	May be used if private secure network.	May be used if private secure network in cases of operational urgency.
Public Telephone, Mobile Telephone and WAP 'phone networks	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used
Pager Systems & SMS	May be used.	Not to be used.	Not to be used.
Facsimile Machines	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used unless encrypted fax service available.
Airwave Radios	May be used.	May be used.	Not to be used unless enhanced end to end encryption service deployed.
Force Data Network, Email Services using PNN – GSI – NHS – CJSM – MOD secure addressing conventions	May be used.	May be used.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.
Internet Email / Internet Services	May be used	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.

If there is a requirement to use any of the above methods of communication at a higher level than recognized safe to do so, the operational urgency and the need for transmission must be weighed against the risk of a security breach, for which the force may be held accountable. If it is decided that such transmissions are essential, they should be kept short and guarded speech used. The use of some form of prearranged codes should be considered to avoid identifying officers, informants or locations.

Requirements and restrictions on the handling/disposal etc of SECRET and TOP SECRET material are not included in this aide-memoire. Should you find yourself confronted with or required to deal with such material, seek advice or assistance from your force Information Security Officer, who will be able to advise you accordingly.

Descriptors

When you originate material requiring a Protective Marking, you **may**, if necessary, add a DESCRIPTOR where it **helps indicate to others** the nature of the sensitivity and the groups of people who need access.

One exception is the PROTECT marking which should always be used with a DESCRIPTOR from the following list:

APPOINTMENTS

Concerning actual or potential appointments that have not yet been announced

HONOURS

Unannounced recognition for exceptional Achievement

MANAGEMENT

Policy and planning affecting the interest of groups of staff

MEDICAL

Medical reports, records and material relating to staff

PERSONAL

Material intended for the person to whom it may be addressed

STAFF

Concerning references to named or identifiable staff or personal confidences entrusted by staff to management

DESCRIPTORS that can be used with either PROTECT or RESTRICTED include:

COMMERCIAL

Relating to a commercial establishments processes or affairs

CONTRACTS

Concerning tenders under consideration and the terms of any tenders

INVESTIGATIONS

Concerning investigations into disciplinary or criminal matters, involving members of the police service

PRIVATE

For information collected through electronic government services provided to the public and agencies and relating to the individual or agencies

Other DESCRIPTORS include:

POLICY

Proposals for new or changed force policy, prior to publication

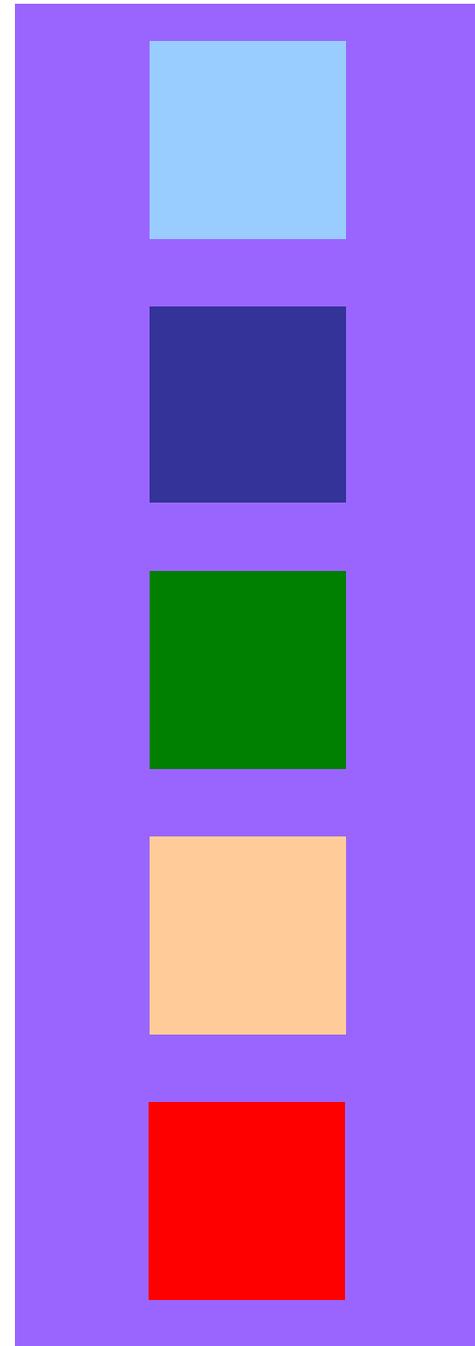
VISITS

Concerning details of visits by, for example, royalty, ministers and other dignitaries.

CHIS

(Covert Human Intelligence Source) regarding informants and their handling. Any informant related information should be protectively marked CONFIDENTIAL as a baseline, with the appropriate handling procedures. Information which identifies an informant should be marked SECRET

With the exception of PERSONAL or PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a protective marking. Special handling instructions may also take the form of caveats, nicknames and code words or exceptionally other handling instructions e.g. DESCRIPTOR may take the form of an operation name – such as - “OPERATION RAINBOW” – EYES ONLY.



This leaflet is designed to inform staff of procedures and help them determine and indicate to others, the levels of protection required when handling official documents.

The term document refers to all material assets, ie papers, drawings, images, disks and all forms of electronic data records. This leaflet is designed as an **aid** only.

Further and more comprehensive guidance can be found in the Manual of Protective Security or from your own **Information Security Officer**.

Vetting Levels

The level of vetting will dictate what protectively marked material can be accessed / handled.

A Basic Check (BC) (Baseline Standard) will allow access to protectively marked information up to CONFIDENTIAL and occasional access to SECRET.

A Security Clearance (SC) (Security Check) is required for individuals who are to be employed in posts where they will have long term, frequent and uncontrolled access to SECRET assets and occasional supervised access to TOP SECRET assets.

A Developed Vetting (DV) clearance is required for those individuals who are to be employed in posts where they will have long term, frequent and uncontrolled access to TOP SECRET assets and includes those while not in such posts that are in a position to directly or indirectly bring about the same degree of damage.

For more detailed information regarding vetting contact your own Vetting Officer.